ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія захисту корпоративної інфраструктури DNS на базі Akamai Edge DNS»

зі спеціальності *125 Кібербезпека*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Аліна ЛИСАЧЕНКО
(підпис)

Виконав: здобувачка вищої освіти групи БСДМ-62
ЛИСАЧЕНКО Аліна
(прізвище, ім'я)

Керівник к.військ.н., доцент ГАХОВ Сергій
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2024

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

API – Application Programming Interface

APT – Advanced Persistent Threat

CDN – Content Delivery Network

CIPS – Cloud Infrastructure and Platform Service

CNAPP – Cloud-Native Application Protection Platform

DDoS – Distributed Denial of Service

DNS – Domain Name System

IaaS – Infrastructure as a Service

IAM – Identity and Access Management

MSSP – Managed Security Service Provider

SASE – Secure Access Service Edge

SOA – Start of Authority

SOC – Security Operations Center

OWASP – Open Web Application Security Project

WAF – Web Application Firewall

ZT – Zero Trust

ВСТУП

Актуальність дослідження. У сучасну цифрову епоху система доменних імен (DNS) є основою глобальної та корпоративних мереж, діючи як транслятор між доменними іменами та IP-адресами. Неправильно налаштований DNS може призвести до збоїв автентифікації, проблем з реплікацією та значного простою. Впровадження ефективних найкращих методів безпеки DNS має важливе значення для захисту корпоративної мережі від потенційних загроз і забезпечення безперебійного обслуговування. Дотримуючись найкращих практик DNS, ми можемо забезпечити безперебійну та безпечну роботу корпоративної мережі, одночасно зменшуючи ризик збоїв. Тому, в загальному процесі забезпечення безпеки інформаційних ресурсів організацій, захист корпоративної інфраструктури DNS займає відповідальне місце.

Вищесказане визначає актуальність теми даної кваліфікаційної роботи, основний зміст якої становлять дослідження технології захисту корпоративної інфраструктури DNS на базі Akamai Edge DNS.

Об'єкт дослідження – захист корпоративної інфраструктури DNS.

Предмет дослідження – технологія захисту корпоративної інфраструктури DNS на базі Akamai Edge DNS.

Мета роботи – розробити порядок застосування технології захисту корпоративної інфраструктури DNS та рекомендації щодо її реалізації.

Наукові завдання:

дослідити сутність проблеми захисту корпоративної інфраструктури DNS;

проаналізувати підходи до захисту корпоративної інфраструктури DNS;

проаналізувати існуючі рішення для захисту корпоративної інфраструктури DNS;

проаналізувати методи та засоби захисту корпоративної інфраструктури DNS на базі Akamai Edge DNS;

розкрити порядок реалізації технології захисту корпоративної інфраструктури DNS на базі Akamai Edge DNS.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

Практичне значення одержаних результатів: запропоновано порядок застосування технології захисту корпоративної інфраструктури DNS на базі Akamai Edge DNS, а також розроблено рекомендації фахівцям з кібербезпеки щодо її реалізації.

Результати кваліфікаційної роботи апробовані на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 25 жовтня 2024 року в Державному університеті інформаційно-комунікаційних технологій, м. Київ.

1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ ЗАХИСТУ КОРПОРАТИВНОЇ ІНФРАСТРУКТУРИ DNS

1.1. Дослідження загроз корпоративній інфраструктурі DNS

Організації стикаються з дедалі більшою кількістю складніших кібератак. Як наслідок, вони все більше визнають важливість використання аналізу загроз і принципів нульової довіри як частини своїх загальних стратегій безпеки. У цьому контексті дані аналізу загроз DNS визнаються надзвичайно цінним і ефективним джерелом інформації для організацій, які прагнуть посилити захист своєї кібербезпеки [1].

В [1] зазначається, що підприємствам необхідно розглядати комплексну безпеку DNS і розвивати свою інфраструктуру безпеки для досягнення цілісного та більш інтегрованого підходу. Консолідація даних про загрози DNS і можливості спостереження в екосистемі безпеки забезпечує проактивний захист, зменшує кіберзагрози та покращує захист. Використовуючи дані аналізу загроз DNS, організації можуть отримати більш глибоке розуміння потенційних загроз і вживати профілактичних заходів для зниження ризику, роблячи DNS ключовим компонентом будь-якої комплексної стратегії кібербезпеки.

Враховуючи важливу роль DNS у функціонуванні Інтернету та корпоративних мереж, а також його потенціал як вектора для найнебезпечніших кібератак (рисунок 1.1), організаціям необхідно віддавати пріоритет безпеці DNS як частині своєї загальної стратегії кібербезпеки.

Розширення ландшафту загроз і дедалі складніші кібератаки означають, що організації потребують більшої видимості та контролю над мережевою діяльністю. Спеціальне рішення безпеки DNS підвищить рівень безпеки та допоможе запобігти витоку даних та іншим кіберзагрозам, тоді як дані DNS, які можна використовувати для аналізу загроз, можна використовувати [1].

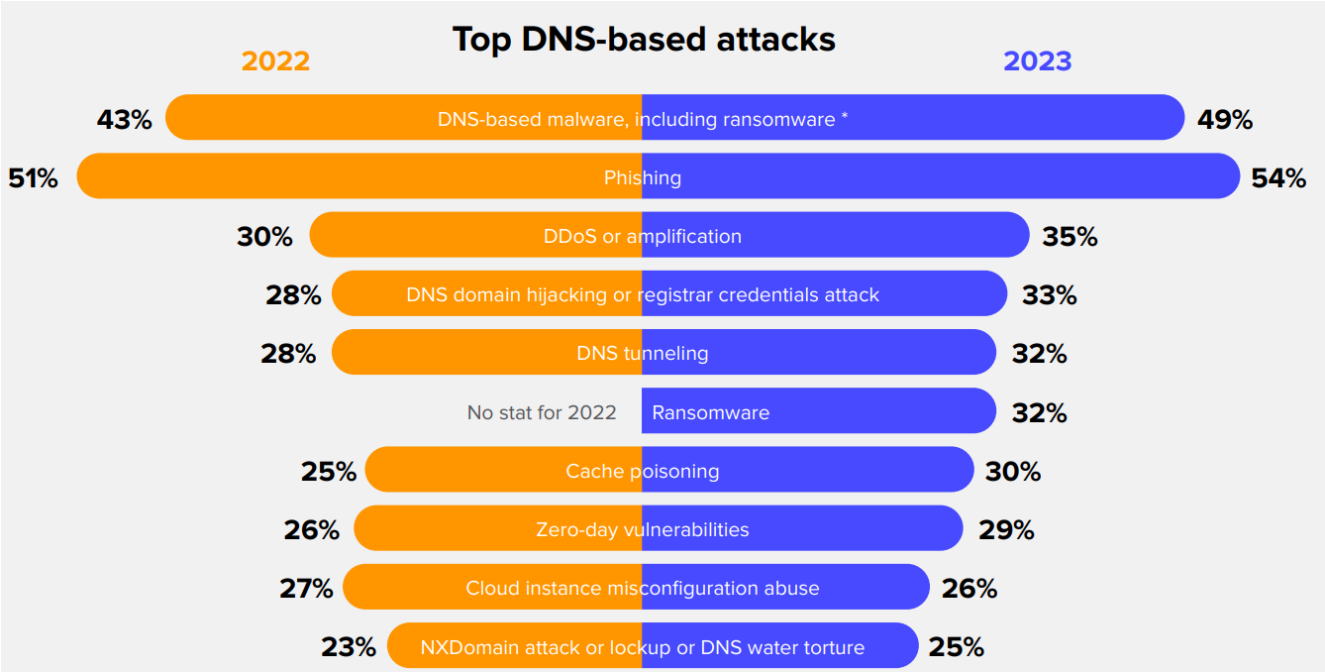

Рис. 1.1. Найпопулярніші атаки на основі DNS [1]

Кібератака на основі DNS може мати значні наслідки як у короткостроковій, так і в довгостроковій перспективі (рисунок 1.2). Одразу після атаки організація може зіткнутися з простоєм або втратою продуктивності внаслідок вимкнення систем або неможливості співробітниками отримати доступ до важливих даних або додатків, що призводить до втрати прибутку, порушення термінів, шкоди репутації та штрафів з боку регуляторів.

Довгостроковий вплив на організацію включає шкоду репутації бренду, втрату клієнтів і зменшення частки ринку. Крім того, успішна атака може призвести до викрадення конфіденційних даних, у тому числі інтелектуальної власності або фінансової інформації, що може призвести до подальших фінансових втрат або юридичної відповідальності.

Для справжнього захисту від кіберзагроз організаціям потрібна служба DNS, здатна виконувати надійні завдання безпеки в режимі реального часу: захист від шкідливих доменів, а також захист користувачів, програм і даних із гарантією повної безперервності обслуговування. Крім того, DNS є важливим джерелом аналізу загроз, надаючи інформацію про підозрілі доменні імена, IP-адреси та інші показники компрометації [1].

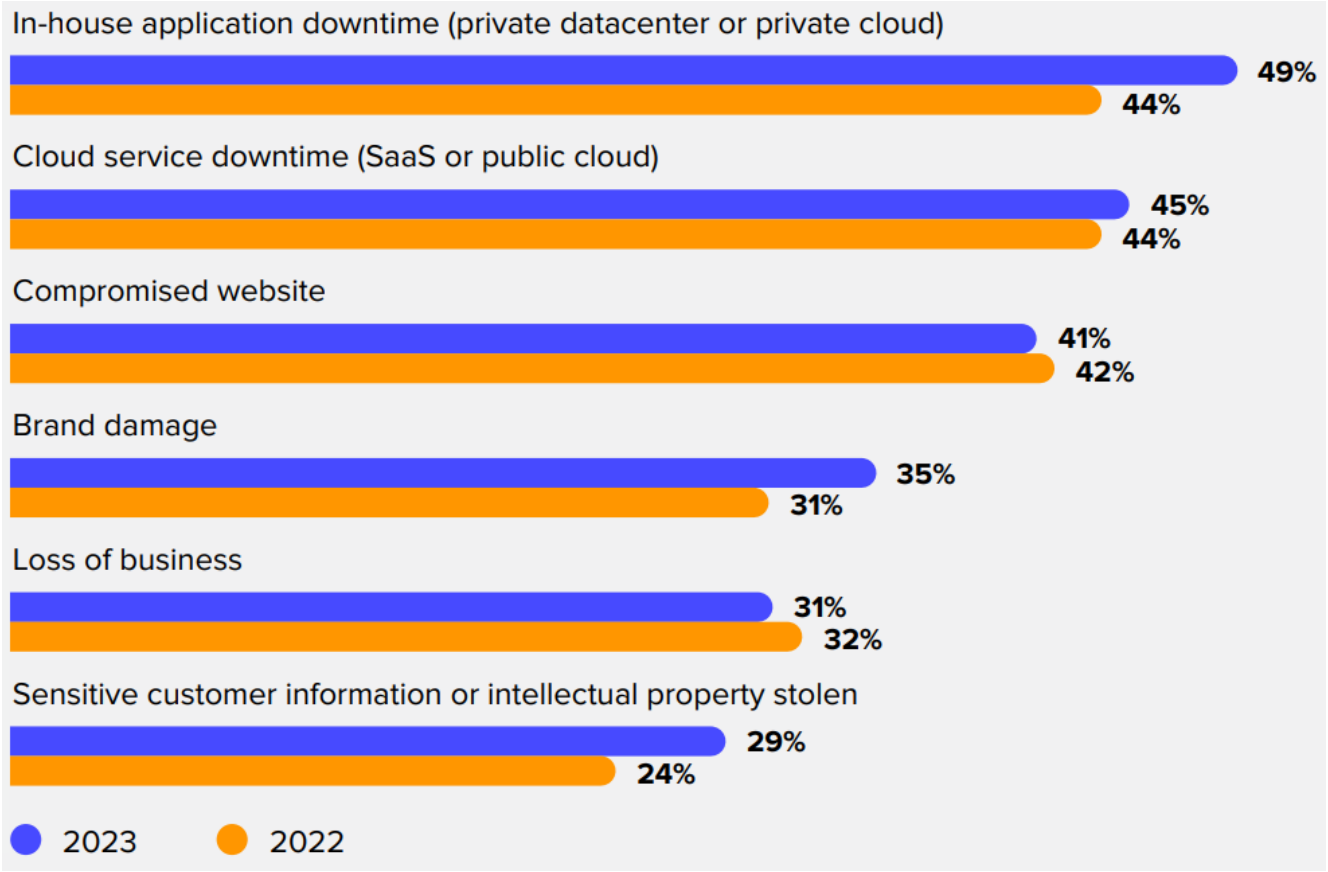

Рис. 1.2. Вплив атак на основі DNS [1]

Враховуючи мінливий ландшафт загроз і різноманітність інфраструктури, організаціям необхідно розвивати свою інфраструктуру безпеки та прийняти більш цілісний, заснований на ризиках і комплексний підхід. У своїй стратегії їм потрібно охопити всі аспекти: різноманітність інфраструктур і пристроїв, різноманітність працівників, будь-які вихідні джерела даних і зміцнення своєї безпеки за допомогою більш інтегрованих і взаємодоповнюючих моделей, що включають нульову довіру та SASE.

В [2, 3] визначено такі найбільші ризики безпеці інфраструктурі DNS у 2024 році:

підробка DNS і отруєння кешу. Підробка DNS, також відома як отруєння кешу DNS, це атака, під час якої пошкоджені дані DNS вставляються в кеш DNS-розпізнавача, що змушує розпізнавач повертати неправильну IP-адресу. Це перенаправляє користувачів на шкідливі сайти без їх відома, що потенційно може призвести до крадіжки даних, зараження зловмисним програмним забезпеченням

та інших порушень безпеки.

Як це працює:

маніпуляції із записами DNS: зловмисники перехоплюють і змінюють відповіді DNS, щоб спрямовувати користувачів на шахрайські сайти;

пошкодження кешу DNS: шкідливі дані вставляються в кеш DNS-сервера, який потім повертає користувачам неправдиву інформацію.

DDoS-атаки на DNS-сервери. Атаки розподіленої відмови в обслуговуванні (DDoS) переповнюють DNS-сервери величезною кількістю запитів, через що вони перестають відповідати та порушують доступ до веб-сайтів і онлайн-сервісів. Ці атаки особливо ефективні, оскільки DNS-сервери є критично важливими для функціональності Інтернету, а статистика за 2023 рік показує, що кількість DDoS-атак подвоїться з 7,9 мільйона до 15,4 мільйона порівняно з 2017 роком.

Як це працює:

затоплення DNS-серверів: зловмисники використовують ботнети, щоб надсилати величезну кількість запитів на DNS-сервер;

вичерпні ресурси: ресурси сервера вичерпані, що призводить до простою служби або зниження продуктивності.

DNS-тунелювання та викрадання даних. Тунелювання DNS – це складний метод атаки, який використовує протокол DNS для тунелювання несанкціонованих даних або створення прихованих каналів зв’язку. Він передбачає кодування даних у запитах і відповідях DNS, що дозволяє зловмисникам обійти традиційні заходи безпеки, такі як брандмауери та системи виявлення вторгнень. Цю техніку можна використовувати для різноманітних зловмисних цілей, включаючи викрадання даних, зв’язок командування та контролю (C2) та обхід мережевих обмежень.

Як це працює:

кодування даних у запитах DNS: зловмисники кодують дані, які вони хочуть отримати, у запитах DNS. Ці запити надсилаються на скомпрометований або контрольований зловмисником DNS-сервер;

декодування з боку зловмисника: DNS-сервер зловмисника отримує закодовані запити, витягує дані та надсилає закодовані відповіді на

скомпрометовану машину;

встановлення каналів C2: Тунелювання DNS також можна використовувати для встановлення каналів C2, дозволяючи зловмисним програмам спілкуватися з віддаленими серверами через трафік DNS.

викрадення та перенаправлення DNS. Викрадення DNS включає контроль над DNS-сервером або зміну записів DNS для перенаправлення трафіку на шкідливі сайти. Цього можна досягти за допомогою різних методів, включаючи порушення налаштувань DNS на маршрутизаторах або маніпулювання записами DNS на рівні реєстратора.

Як це працює:

порушення налаштувань DNS: зловмисники отримують доступ до налаштувань DNS і змінюють їх, щоб вказувати на шкідливі IP-адреси;

маніпулювання записами реєстратора: DNS-записи змінюються на реєстраторі домену, перенаправляючи трафік на сайти, контрольовані зловмисниками.

атаки «людина посередині» на DNS. Під час атаки «людина посередині» (MitM) зловмисники перехоплюють і змінюють DNS-зв'язок між користувачем і сервером DNS. Це дозволяє їм перенаправляти користувачів на шкідливі сайти або маніпулювати відповідями DNS для сприяння іншим типам атак.

Як це працює:

перехоплення трафіку DNS: зловмисники розташовуються між користувачем і сервером DNS, перехоплюючи запити та відповіді DNS;

зміна відповідей DNS: відповіді DNS змінюються для перенаправлення користувачів або надання неправильної інформації.

атаки на перепризв'язування DNS. Атаки повторного прив'язування DNS використовують систему DNS для обходу політики того самого джерела у веб-браузерах, дозволяючи зловмисникам взаємодіяти з внутрішніми мережевими службами. Це може призвести до несанкціонованого доступу та маніпулювання внутрішніми системами.

Як це працює:

повторне прив’язування відповідей DNS: зловмисник обманом змушує браузер жертви неодноразово перетворювати доменне ім’я на різні IP-адреси, включно з адресами внутрішньої мережі;

обхід політики того самого походження: атака використовує політику того самого походження браузера для доступу до внутрішніх служб.

вразливості протоколів DNS. Сам протокол DNS може мати вразливості, якими зловмисники можуть спричинити різноманітні проблеми безпеки. Ці вразливості можуть бути притаманними протоколу або результатом неправильної реалізації.

Як це працює:

використання недоліків протоколу: зловмисники використовують слабкі місця в протоколі DNS або його реалізації;

створення зловмисних DNS-запитів: спеціально створені DNS-запити використовуються для використання вразливостей у програмному забезпеченні DNS.

Також авторами [2] визначено нові загрози DNS:

атаки посилення DNS. Атаки посилення DNS є різновидом DDoS-атак. У 4 кварталі 2023 року експерти спостерігали зростання кількості таких атак на 117% порівняно з минулим роком. У ньому зловмисники використовують відкритий характер DNS-серверів, щоб наповнити ціль величезною кількістю трафіку.

Ця атака використовує невідповідність між малим розміром DNS-запиту та значно більшим розміром відповіді. Надсилаючи невеликий запит із підробленою IP-адресою на DNS-сервер, зловмисники можуть посилити відповідь, викликаючи значне навантаження трафіку на цільовий сервер.

Як це працює:

підробка запитів: зловмисники надсилають DNS-запити з IP-адресою цілі, змушуючи DNS-сервер замість цього надсилати відповіді цілі;

посилення трафіку: великий розмір відповідей DNS порівняно із запитами створює ефект посилення, перевантажуючи ціль надмірним трафіком.

розповсюдження шкідливих програм на основі DNS. У 2023 році 38% DNS-

атак стосувалися розповсюдження шкідливого програмного забезпечення на основі DNS. Це свідчить про те, що DNS все частіше використовується як вектор розповсюдження шкідливих програм. Зловмисники використовують DNS-запити для доставки зловмисного корисного навантаження, використовуючи надійний характер трафіку DNS для обходу заходів безпеки. Цей метод особливо підступний, оскільки трафік DNS часто пропускається через брандмауери без перевірки, забезпечуючи прихований канал для розповсюдження зловмисного програмного забезпечення.

Як це працює:

шкідливі DNS-відповіді: зловмисники налаштовують зловмисні DNS-сервери, щоб відповідати IP-адресами, на яких розміщено зловмисне програмне забезпечення;

доставка корисного навантаження: коли користувачі неусвідомлено запитують ці зловмисні сервери, вони перенаправляються на сайти, які автоматично завантажують і встановлюють шкідливі програми.

DNS-атаки на основі ШІ. Згідно з новим звітом Sapio Research і Deep Instinct, 75% спеціалістів із безпеки повідомили про зростання кількості атак за останній рік, причому 85% пов’язують це зростання зловмисниками, які використовують генеративний ШІ. Інтеграція ШІ в кібератаки призвела до появи DNS-атак на основі ШІ. Ці атаки використовують алгоритми машинного навчання для динамічної адаптації та уникнення виявлення, що робить їх ефективнішими та складнішими для подолання. Штучний інтелект можна використовувати для автоматизації та оптимізації стратегій DNS-атак, підвищуючи рівень успішності.

Як це працює:

адаптивні стратегії атак: алгоритми ШІ аналізують захист мережі та адаптують стратегії атак у режимі реального часу, щоб обійти заходи безпеки;

автоматизоване виконання: штучний інтелект автоматизує виконання складних DNS-атак, таких як тунелювання, посилення та підробка, що робить їх ефективнішими та важчими для виявлення.

гібридні DNS-атаки. Гібридні DNS-атаки поєднують кілька методів DNS-

атак для створення більш складних і ефективних загроз. Інтегруючи такі методи, як спуфінг, тунелювання та посилення, зловмисники можуть досягти більшого впливу та успішніше уникати виявлення.

Як це працює:

комбінування методів: зловмисники об’єднують різні методи атак DNS, щоб використовувати кілька вразливостей одночасно;

підвищене ухилення: використання кількох методів ускладнює системам безпеки виявлення та пом’якшення всіх аспектів атаки.

Необхідно зазначити, що інфраструктура DNS підходить для таких ключових стратегій безпеки [1]:

розвідка загроз: DNS можна використовувати для відстежувати та блокувати доступ до відомих шкідливих доменів, допомагаючи запобігти зараженню зловмисним програмним забезпеченням та іншим типам кібератак;

забезпечення нульової довіри та доступу до мережі без довіри: DNS можна використовувати для забезпечення безпечного доступу до ресурсів компанії за допомогою засобів керування безпекою на основі DNS, щоб гарантувати, що лише авторизовані користувачі та пристрої мають доступ до цих ресурсів. Це включає мікросегментацію, керовану політиками на основі DNS, щоб дозволити точне керування доступом;

граничний сервіс безпечного доступу (SASE):DNS можна використовувати як частину хмарного рішення безпеки для надання безпечних служб веб-шлюзу, таких як фільтрація URL-адрес і перевірка вмісту;

пристрої IoT: DNS можна використовувати для керування та захисту пристроїв IoT для доступу лише до їхніх внутрішніх ресурсів за допомогою фільтрації списку дозволених ресурсів;

центр обробки даних і хмара: DNS можна використовувати в контролі доступу до додатків, захисті безперервності обслуговування та виявленні загроз.

Розвідка про загрози стала ключовим аспектом захисту кібербезпеки, і 60% організацій вважають її життєво необхідною для стратегії компанії та захисту від кібератак. Причин багато і різноманітні: кіберзлочинці монетизують успішні атаки

за допомогою різних засобів, зокрема програм-вимагачів, витоку стратегічних даних, шкоди репутації бренду та продажу інтелектуальної власності, підкреслюючи необхідність аналізу своїх мотивів і цілей – своїх намірів. Спостерігаючи за моделями та діями суб'єктів загрози – їхньою поведінкою – організації можуть покращити свою здатність проактивно виявляти та пом'якшувати загрози. DNS може надати організації з цінними можливостями аналізу загроз шляхом аналізу трафіку DNS на шаблони та індикатори компрометації.

Захист сучасних IT-середовищ потребує вирішення проблем, пов'язаних зі складністю (кількістю пристроїв, програм, типів даних і мережевих архітектур), масштабом (розгортання хмари та Інтернету речей), видимістю (численні пристрої та кінцеві точки, що генерують величезні обсяги даних) і контролем доступу (хмарні служби, пристрої Інтернету речей, віддалені працівники та працівники в роумінгу). Організації повинні впроваджувати надійні, консолідовані політики безпеки та засоби контролю в розширеному підприємстві, щоб пом'якшити ці виклики та забезпечити безпеку їхніх додатків, служб, користувачів та IT-середовища.

Безпека DNS приватного підприємства приносить значні переваги розширеному підприємству, забезпечуючи повну видимість і контроль над мережевим трафіком. Організації можуть захистити свої дані, користувачів і активи від складних загроз за допомогою однакових політик і функцій безпеки, незалежно від того, де вони розташовані.

Нульова довіра (Zero Trust) використовується для протидії сучасним кіберзагрозам за допомогою проактивного підходу до безпеки, заснованого на доступі з найменшими привілеями. При правильній реалізації за допомогою багаторівневої стратегії захисту модель ZT забезпечує надійну безпеку та зміцнює кіберстійкість бізнесу, дозволяючи лише перевіреним користувачам із авторизованими пристроями отримувати постійний доступ до ресурсів.

Принципи ZT і SASE доповнюють один одного: ZT забезпечує безпеку контролю доступу, тоді як SASE пропонує мережеву архітектуру для

впровадження та виконання політик ZT. Поєднання цих двох створює модель безпеки, яка забезпечує безпечний доступ до програм і даних, вирішуючи проблеми безпеки розподіленої та віддаленої робочої сили та все більшого використання хмарних програм і служб. DNS пропонує просту відправну точку на вашому шляху до нульової довіри Однак впровадження ZT стикається зі складними проблемами через розгалужені IT-сфери, застарілі технології, численні постачальники безпеки та різні хмарні платформи [1].

Організації застосовують більш проактивний підхід до безпеки, заздалегідь визначаючи потенційні загрози та вразливі місця та вживаючи заходів для їх запобігання. Перехід від реактивного захисту до проактивного вимагає інтегрованого підходу до безпеки. DNS є фундаментальним компонентом цього підходу, особливо коли цінні дані DNS надаються системам безпеки, таким як інформація про безпеку та керування подіями (SIEM) або оркестрування безпеки, автоматизація та відповідь (SOAR) через відкриті API.

Аналіз трафіку DNS допомагає виявити незвичайні шаблони трафіку, відкриваючи, наприклад, шкідливі домени нульового дня, які використовуються для викрадання даних програмами-вимагачами.

DNS фільтрація це ефективний спосіб заблокувати доступ до відомих зловмисних доменів і запобігти зв’язку програм-вимагачів із серверами командування та керування (C&C), запобігаючи атаці до того, як вона завдасть будь-якої шкоди. Фільтрацію DNS також можна використовувати для блокування доступу до відомих фішингових сайтів, що може в першу чергу запобігти атакам програм-вимагачів.

Використовуючи аналіз і фільтрацію трафіку DNS у поєднанні з іншими технологіями безпеки, організації можуть виявляти спроби несанкціонованого доступу та швидко реагувати на атаки програм-вимагачів, мінімізуючи потенційну шкоду репутації та знижуючи ризики фінансових втрат.

Незважаючи на те, що 80% організацій визнають, що безпека DNS є критично важливою, інвестиції в знання та використання DNS залишаються тривожно низькими. Витрати та наслідки DNS-атак рік за роком продовжують завдавати

серйозної шкоди.

Через важливість протоколу DNS у сучасному середовищі загроз потрібна спеціальна розвідка про загрози DNS. Щоб посилити захист мережі, необхідно краще використовувати інструменти безпеки DNS і актуальні дані для забезпечення проактивного захисту та раннього виявлення загроз, безпечного підключення для роботи з будь-якого місця та бути простою відправною точкою для стратегій нульової довіри.

Отже, DNS відіграє важливу роль у впровадженні різних концепцій безпеки, допомагаючи захистити організації від ландшафту загроз і забезпечити безпеку їхніх ресурсів: користувачів, пристроїв, додатків і служб.

1.2. Аналіз підходів до захисту корпоративної інфраструктури DNS

DNS означає систему доменних імен. Це система, яка перетворює доменні імена в IP-адреси, які комп’ютери використовують для ідентифікації один одного в Інтернеті. Коли ми вводимо URL-адресу у веб-переглядачі, наш комп’ютер надсилає DNS-серверу запит на пошук IP-адреси, пов’язаної з цим доменним іменем. Потім DNS-сервер надсилає IP-адресу назад на ваш комп’ютер, дозволяючи йому підключитися до веб-сайту. DNS працює через ієрархію серверів, при цьому сервери верхнього рівня містять інформацію про кореневі доменні імена (наприклад, .com, .org тощо), а сервери нижчого рівня містять інформацію про конкретні доменні імена. Це дозволяє ефективно та точно перекладати доменні імена в IP-адреси, що є важливим для функціонування Інтернету. Без DNS Інтернет, яким ми його знаємо, був би неможливий [3].

Система DNS є вразливою до численних кіберзагроз через її конструктивні обмеження та відсутність заходів безпеки. Такі небезпеки включають спуфінг, посилення, DoS та перехоплення приватної інформації. Крім того, DNS-атаки часто використовуються як тактика відволікання разом з іншими кібератаками, що ускладнює групі безпеки зосередитися на потенційно більш серйозній загрозі. З огляду на ці вразливості, дуже важливо мати надійну безпеку DNS, щоб запобігти

DNS-атакам і захистити безперервність бізнесу.

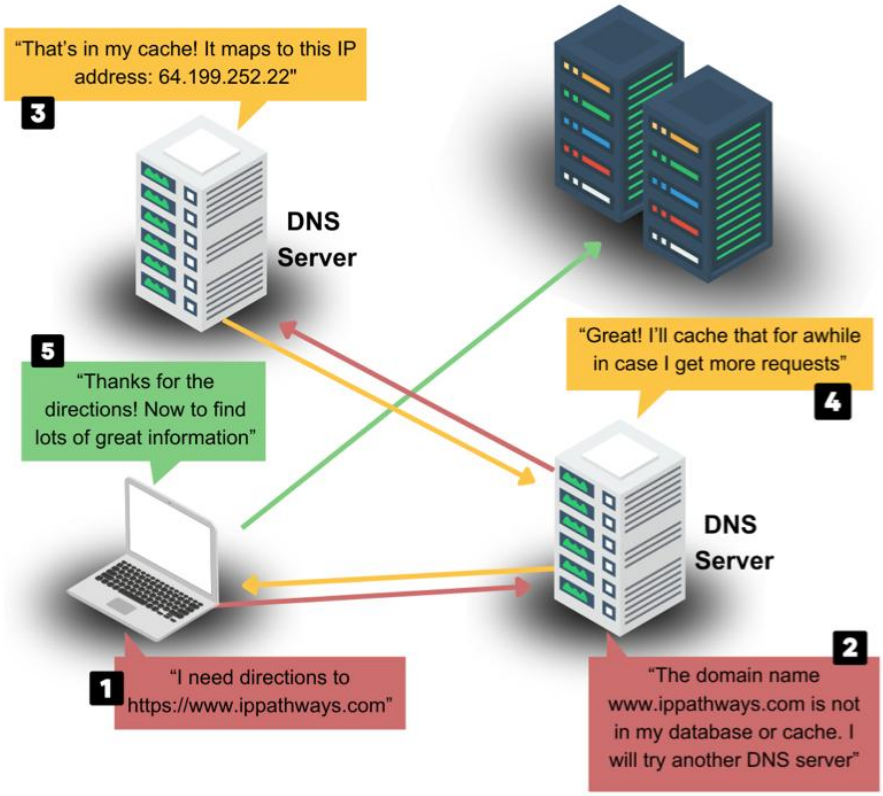

Рис. 1.3. Принцип роботи системи доменних імен [3]

Система доменних імен (DNS) це розподілена обчислювальна система, яка забезпечує доступ до Інтернет-ресурсів за допомогою зручних доменних імен, а не IP-адрес, шляхом перекладу доменних імен на IP-адреси та назад [9].

Інфраструктура DNS складається з обчислювальних і комунікаційних об'єктів, які називаються серверами імен, кожен з яких містить інформацію про невелику частину простору доменних імен. Дані про доменне ім'я, які надає DNS, призначені для доступу до будь-якого комп'ютера, розташованого будь-де в Інтернеті.

Оскільки дані DNS призначені для загального доступу, зберігаючи конфіденційність даних DNS. Основними цілями безпеки для DNS є цілісність даних і автентифікація джерела, які необхідні для забезпечення автентичності інформації про доменне ім'я та збереження цілісності інформації про доменне ім'я під час передачі [9].

Компоненти DNS часто зазнають атак типу «відмова в обслуговуванні», спрямованих на порушення доступу до ресурсів, доменні імена яких обробляються атакованими компонентами DNS [9].

Перш ніж визначити цілі безпеки, необхідно визначити будівельні блоки DNS. DNS включає такі об’єкти [9]:

платформу (апаратне забезпечення та операційну систему), на якій розміщено сервер імен і резолвер;

сервер імен і програмне забезпечення резолвера;

DNS-транзакції;

базу даних DNS (файли зон);

файли конфігурації в сервері імен і резолвері.

Мережна технологія рівня доступу до медіа (тобто мережа Ethernet, що з’єднує розпізнавач заглушки та локальний сервер розпізнавання імен) не входить у визначення DNS.

Конфіденційність, цілісність, доступність і автентифікація джерела є цілями безпеки, які є спільними для будь-якої електронної системи. Однак очікується, що DNS надасть інформацію про розпізнавання імен для будь-якого загальнодоступного Інтернет-ресурсу. Таким чином, за винятком даних DNS, що стосуються внутрішніх ресурсів (наприклад, серверів усередині брандмауера тощо), які надаються внутрішніми серверами імен DNS через безпечні канали, дані DNS, надані загальнодоступними серверами імен DNS, не вважаються конфіденційними [9].

Отже, конфіденційність не є однією з цілей безпеки DNS. Забезпечення автентичності інформації та підтримання цілісності інформації, що передається, має вирішальне значення для ефективного функціонування Інтернету, для якого DNS надає службу розпізнавання імен.

Отже, цілісність і автентифікація джерела є основними цілями безпеки DNS. Через величезну різноманітність платформ серверів імен і базових мереж, у яких знаходяться компоненти DNS (такі як програмне забезпечення сервера імен і програмне забезпечення розпізнавача), неможливо запобігти всім типам атак на

відмову в обслуговуванні. Однак необхідно дотримуватися деяких базових вказівок, щоб запобігти атакам на відмову в обслуговуванні, які використовують уразливості в платформі сервера імен, вмісті даних файлу зони та конфігурації контролю доступу для певних транзакцій DNS [9].

У передовій архітектурі DNS клієнти вказують на внутрішній рекурсивний рівень DNS для вирішення DNS (рисунок 1.4). На цьому рівні клієнт запитує внутрішній рекурсивний рівень, який рекурсує (всередині або ззовні), щоб знайти результат. Потім цей результат кешується локально протягом заданого «часу життя» (TTL). Оскільки результати кешуються локально, і це перша (і єдина) точка контакту клієнта зі службою DNS, більша частина ємності (запитів на секунду) буде тут.

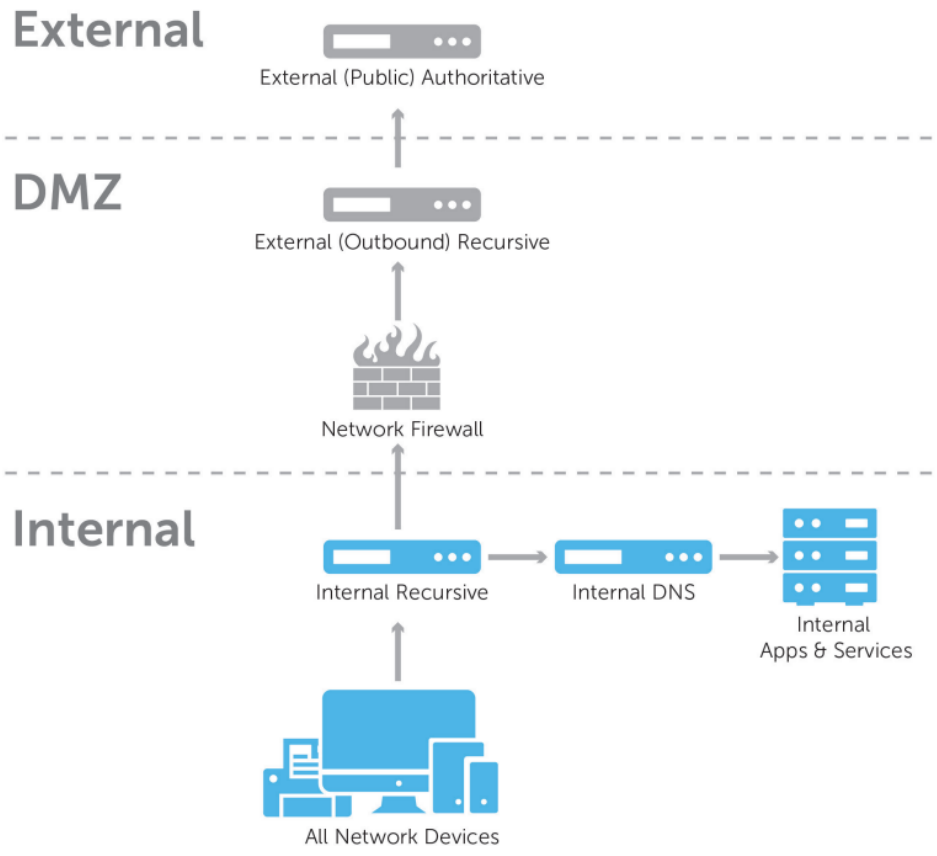

Рис. 1.4. Внутрішній рекурсивний рівень DNS [8]

Як правило, цей рівень не містить фактичних даних DNS – це лише конфігурація. Внутрішній рекурсивний рівень виконує пошук, якщо будьякий

інший компонент служби DNS виходить з ладу. Слід також зазначити, що терміни «рівень кешування» та «внутрішній рекурсивний рівень» часто використовуються як синоніми.

Зовнішній рекурсивний рівень (рисунок 1.5) обробляє вихідні запити до Інтернету. Якщо внутрішній рекурсивний рівень не може знайти достовірну відповідь на запит DNS, він перешле запит на зовнішній рекурсивний рівень для вирішення в Інтернеті. Оскільки ці модулі бачитимуть лише запити, пов'язані з Інтернетом, зовнішні рекурсивні сервери повинні знаходитися в DMZ.

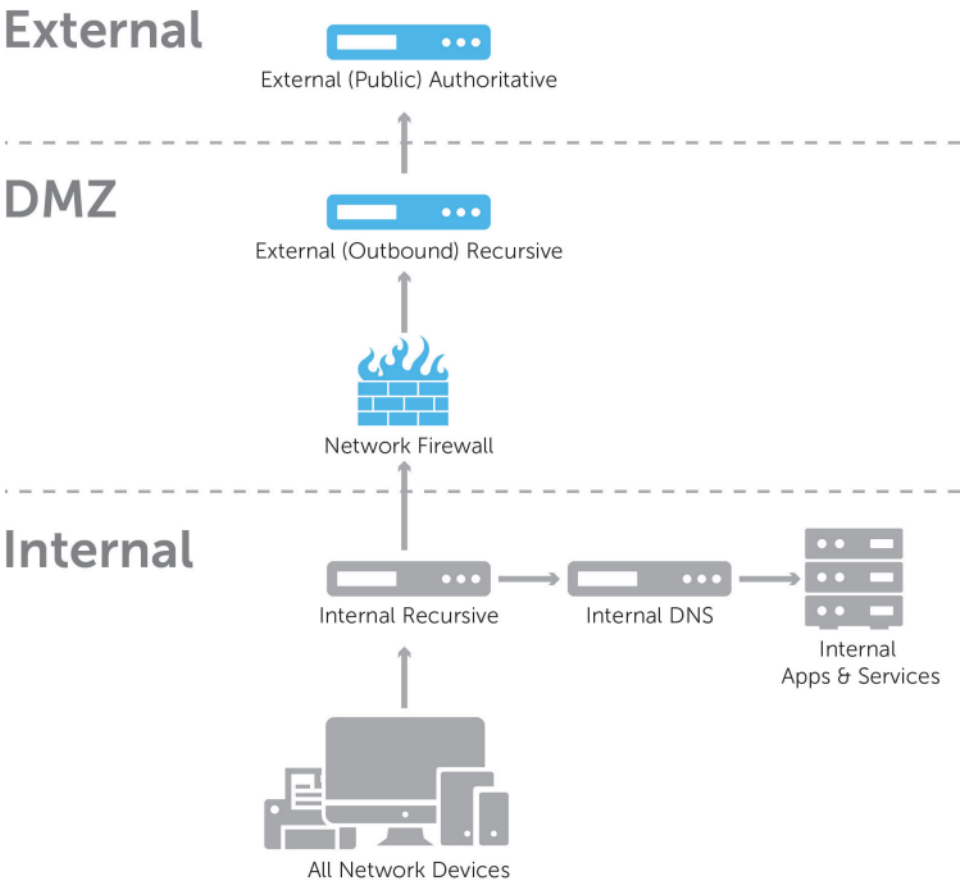

Рис. 1.5. Зовнішній рекурсивний рівень DNS [8]

Першою перевагою є перевірка DNSSEC, де єдиними запитами, перевіреними для DNSSEC, є вихідні Інтернет-запити. Безпека є важливою мірою для зовнішнього рекурсивного рівня. Відповіді DNS, по суті, є запрошенням повернутися до мережі. Якщо ці відповіді захоплені зловмисником, використання зовнішнього рекурсивного рівня «захопить» цю відповідь у DMZ, а не поверне

безпосередньо до внутрішнього простору імен DNS. Оскільки доступ до внутрішнього DNS простір імен можна використовувати для створення карти мережі шляхом розшифровки політик імен DNS, дуже важливо створити рівень безпеки для захисту від загроз для цієї області мережі.

Безпека DNS має вирішальне значення для захисту мереж і користувачів від кіберзагроз. DNSSEC, фільтрація DNS, брандмауери DNS, аудити DNS і виявлення аномалій є одними з найефективніших методів безпеки DNS, які можуть допомогти вам захистити мережу від атак. Впроваджуючи ці заходи, ви можете забезпечити автентичність, цілісність і доступність служб DNS і захистити свою мережу від кіберзлочинців [8].

В [2] зазначаються такі основні рішення, які ми можемо застосувати, щоб захистити свою організацію:

впровадження DNSSEC (розширення безпеки DNS): використовує цифрові підписи для перевірки даних DNS, запобігаючи спуфінгу та отруєнню кешу;

використання фільтрації та блокування DNS: аналізує та блокує шкідливі домени для захисту від фішингу та зловмисного програмного забезпечення;

моніторинг і реєстрація трафіку DNS: безперервно відстежує та аналізує трафік DNS для виявлення підозрілих дій і реагування на них;

безпечне налаштування DNS-серверів: захищає DNS-сервери за допомогою посилення, контролю доступу та безпечних протоколів для зменшення вразливості;

використання багаторівневих стратегій безпеки: поєднує різні заходи безпеки для створення надійного захисту від атак DNS;

вибір правильного програмного забезпечення DNS: вибір програмного забезпечення DNS із розширеними функціями безпеки, масштабованістю та надійністю для оптимального захисту.

Вплив на бізнес, спричинене атаками, націленими на DNS, може призвести до того, що компанію неможливо знайти в цифровому середовищі. Крім того, існує великий вплив, який зазнає ця компанія через її недоступність, що шкодить її іміджу на ринку та сприйняттю споживачів [4].

У той час як з одного боку екрана користувач отримує сповіщення про

недоступний DNS-сервер або збій DNS, з іншого боку компанія більше не доступна та невидима для потенційних споживачів. Фінансовий вплив, викликаний цією проблемою, є величезним і навіть може бути незворотним залежно від збитків організації [4].

Основні підходи, які можна використовувати для захисту DNS [4]:

DNS захист від DDoS. Як частина пакету запобігання DDoS, захист DNS спрямований на те, щоб інфраструктура та послуги, які пропонує компанія, залишалися доступними. Цей інструмент потрібно вибирати ретельно, враховуючи, що помилкові спрацьовування мають величезний вплив на компанію.

Цей моніторинг необхідно впроваджувати разом із моделюванням трафіку вашої компанії, захищаючи ваші послуги та гарантуючи лише законний трафік запитів. Ефективний інструмент моніторингу зможе відрізнити легітимних і нелегітимних користувачів, запобігаючи неналежному доступу та розпізнаючи шаблони атак нульового дня.

DNSSEC (Domain Name System Security Extensions) це інструмент безпеки, який допомагає додати рівень захисту до системи DNS. Ця функція працює шляхом цифрового підпису записів DNS, запобігаючи їх підробці або зміні під час передачі інформації.

Діючи на випередження, ця система запобігатиме перенаправленню трафіку intermed на сторінки зі зловмисним вмістом або загрозами на основі DNS і пастками, такими як фішинг . Таким чином ваша компанія підвищить автентичність і цілісність DNS, запобігаючи маніпуляціям і перенаправленням.

DNS-фільтр дозволяє більш наполегливо відстежувати та контролювати веб-трафік. Використовуючи DNS для блокування шкідливих сторінок і фільтрації небезпечного вмісту, цей інструмент допомагає підвищити безпеку даних у компанії та гарантує більш повний контроль над вмістом , доступ до якого здійснюється в робочому середовищі.

Використовуючи цю функцію, ваша компанія зможе запобігти виникненню проблем у фішингових електронних листах, пастках, присутніх на шкідливих сторінках, і вмісті, який становить певний ризик. Таким чином ваш підхід до

безпеки буде більш повним і наполегливим.

Брандмауер це функція безпеки, яка дозволяє контролювати вхідний і вихідний трафік і блокувати трафік на основі попередньо встановлених правил безпеки. Завдяки своїй функціональності брандмауер є одним із основних ресурсів, що використовуються в кібербезпеці в останні десятиліття, що дозволяє розміщувати захисний бар'єр між мережами.

Залежно від мети та стратегії безпеки компанії ви можете вибрати певний брандмауер, наприклад проксі-брандмауер, уніфікований брандмауер керування загрозами, брандмауер наступного покоління тощо. Вибір ідеального інструменту має ґрунтуватися на потребах вашої компанії та загрозах, які можуть зашкодити автентичності та безпеці бізнесу.

Постійний моніторинг інфраструктури DNS. Враховуючи важливість DNS у функціональності під час виконання численних завдань у цифровому середовищі, постійний моніторинг є важливим для підвищення захисту вашої компанії. Методи моніторингу продовжують допомагати оптимізувати безпеку бізнесу та завчасно виявляти можливі нетипові чи зловмисні дії.

Беручи до уваги, що кіберзлочинці впроваджують все більш ефективні стратегії для проникнення в системи вашої компанії, цей моніторинг стає незамінним фактором. Використовуючи надійний інструмент, компанія може бути на крок попереду та гарантувати, що її ресурси та інформація залишатимуться захищеними.

Дуже важливо встановити позицію запобігання загрозам на основі DNS. Це означає, що не просто вирішувати проблеми, коли вони виникають, необхідно підготуватися до боротьби з цими загрозами і, що найважливіше, запобігати їх виникненню.

Інструменти моніторингу допоможуть генерувати сповіщення про підозрілу діяльність і забезпечать блокування цих проблем до того, як вони завдадуть будь-якої шкоди бізнесу. Таким чином ваша стратегія безпеки буде зміцнена, і ваша компанія зможе забезпечувати ще більше безпеки для всіх користувачів, співавторів, партнерів і багато іншого.

Збереження конфіденційності за допомогою інновацій DNS. Технологічний прогрес дозволив розробити спеціальні інструменти, які гарантують, що DNS є захищеним і ефективним ресурсом. Переклад, здійснений системою DNS, дозволяє нам легко отримувати доступ до сторінок , однак є аспекти безпеки, які необхідно посилити, щоб гарантувати захист цього ресурсу.

Системне шифрування DNS працює на основі двох стандартів [4]:

DNS через TLS, або DoT, це стандарт шифрування запитів DNS, спрямований на підвищення захисту. Ця система використовує протокол безпеки TLS, розроблений для шифрування та автентифікації комунікацій, що здійснюються в цифровому середовищі.

Також відомий як SSL, TLS гарантує, що кіберзлочинці не перехоплять, не підроблять і не змінять запити та відповіді DNS. Основою цього інструменту є протокол UDP (User Datagram Protocol).

DNS через HTTPS (DoH). Цей тип шифрування представляє себе як альтернативу DoT (DNS через TLS). У цьому випадку запити також проходять шифрування, але надсилаються через протоколи HTTP або HTTP/2. Це означає, що вони не надсилаються безпосередньо через UDP.

Однак він працює так само, як і DoT, не даючи кіберзлочинцям зламати, змінювати або підробляти трафік DNS. DNS через HTTPs також додає додатковий рівень безпеки мережам і запобігає будь-якому маніпулюванню ними з боку злочинців.

Контроль доступу та надійні стратегії автентифікації. Враховуючи величезний вплив загроз на основі DNS і дій кіберзлочинців на компанію, надзвичайно важливо забезпечити більш ефективну стратегію безпеки. Функції безпеки, які протягом тривалого часу називалися брандмауером і антивірусом, стали ще складнішими.

Розвиток стратегій, спрямованих на перенаправлення інформації та вторгнення в мережі та пристрої, посилив потребу в більш конкретних інструментах. З цієї причини для захисту мереж і пристроїв компанії важливо застосувати контроль доступу та надійні стратегії автентифікації.

Це означає, що співробітники повинні пройти процес навчання та адаптації, щоб зрозуміти важливість впровадження якісних паролів, щоб запобігти їх легкому виведенню та доступу неавторизованих користувачів. Крім того, дуже важливо застосувати багатофакторну автентифікацію, щоб критично важливі системи компанії залишалися захищеними. У цьому сенсі ми також маємо на увазі DNS-сервери, які, хоча й важливі, також вимагають більш специфічних інструментів захисту.

Контроль доступу також є стратегією, яка може допомогти вашій компанії залишатися захищеною, запобігаючи доступу користувачів до вмісту, який вважається небезпечним або шкідливим. Це пов'язано з тим, що кіберзлочинці, використовуючи недостатню обізнаність користувачів або вилучення, встановлюють цифрові пастки на сторінках, які вважаються нешкідливими, приховуючи шкідливі файли та програми в банерах, посиланнях і навіть підозрілих новинах.

Захист налаштування DNS, щоб мінімізувати ризик. Основною метою налаштування корпоративної системи DNS-сервера є підвищення безпеки та обмеження зловмисного доступу. Щоб досягти цього, є деякі конфігурації, які можна впровадити у компанії для оптимізації захисту:

обмеження зональних трансферів. Передача зони DNS є різновидом транзакції сервера доменних імен. Ця стратегія дозволяє менеджерам тиражувати базу даних DNS на наборі серверів за допомогою протоколу TCP.

Цей механізм використовується для синхронізації оновлених даних на основних DNS-серверах і може працювати двома способами:

передача повної зони (axfr): у цьому випадку основний DNS-сервер сповіщає вторинний DNS-сервер про можливі зміни, внесені до зони. Якщо серійний номер основного DNS перевищує номер у вторинному DNS , файл зони буде скопійовано на вторинні сервери DNS.

інкрементальна передача зони (IXFR): основний DNS-сервер сповіщає вторинний DNS-сервер про зміни, внесені до певної зони. Якщо серійний номер у первинному DNS більший, ніж у вторинному, ці зміни порівнюються, і копіюються

лише записи, які змінилися.

Ми можемо встановити більш безпечну передачу зони за допомогою обмеження IP-адреси або підпису передачі DNS.

Обмеження рекурсії. Обмеження рекурсії не дозволить мережі DNS виконувати рекурсивні запити, запобігаючи відповіді на будь-який запит з будь-якої IP-адреси. Цей захід також запобіжить рекурсивному серверу зберігати підроблені дані, уникаючи направлення користувачів на підроблені веб-сайти або перенаправлення серверів кіберзлочинцями під час кібератак. З цієї причини обмеження рекурсії працює як рівень захисту в мережі DNS. Ця стратегія пом'якшить дії зловмисників і захистить дані.

Вимкнення непотрібних функцій. Очищення непотрібних ресурсів у системі DNS допоможе усунути застарілі записи. Хоча DNS є фундаментальним для використання цифрових ресурсів, він також має непотрібні функції, які можуть збільшити поверхню атаки корпоративної мережі.

Ефективне впровадження DNSSEC у стратегії безпеки. DNSSEC це функція DNS, яка дозволяє додати додатковий рівень безпеки до корпоративного DNS. DNSSEC працює шляхом цифрового підпису записів DNS, щоб запобігти їх модифікації або фальсифікації під час передачі даних. З цієї причини DNSSEC не дозволяє кіберзлочинцям маніпулювати записами DNS і спричиняти проблеми з автентичністю та цілісністю цього ресурсу. Використовуючи ключі для підпису цифрових записів DNS, DNSSEC має на меті переконатися, що записи DNS, які використовуються, збігаються з записами, наданими в доменній зоні серверів.

Впровадження цієї функції безпеки у корпоративній мережі підвищить конфіденційність і безпеку даних, запобігаючи основним кібератакам, спрямованим на DNS, таким як атаки з отруєнням кешу DNS. Завдяки цьому можна дозволити відповідне націлювання на веб-сайти, до яких звертаються користувачі, запобігаючи доступ із нелегітимних сторінок.

Необхідно відмітити вирішальну роль моніторингу трафіку DNS у проактивному виявленні. Протягом багатьох років стратегія цифрової безпеки, яку впроваджували компанії, базувалася на більш реактивному баченні. Це означає, що

замість моніторингу та пом’якшення неналежного доступу використовувалась стратегія полягала у вирішенні проблем у міру їх виникнення.

Розвиток технологій дозволив змінити цю парадигму, змусивши компанії прийняти більш проактивний погляд на виявлення та запобігання загрозам на основі DNS. Інструменти безпеки, спрямовані на моніторинг, впроваджуються, щоб запобігти проблемам безпеки ще до того, як вони виникнуть.

Моніторинг DNS дозволяє виявляти підозрілу активність, неавторизовані зміни та незвичайні запити в цьому інструменті. Таким чином, компанія зможе виявляти загрози на основі DNS, перш ніж вони можуть спричинити проблеми для бізнесу.

Використання брандмауера та DNS-фільтрації може мати фундаментальне значення для посилення стратегії безпеки вашої організації. Ці інструменти дозволяють безперервно контролювати корпоративні цифрові ресурси та гарантують посилення безпеки мереж і пристроїв компанії.

Брандмауер і DNS-фільтр дозволяють здійснювати постійний моніторинг, зосереджуючись на виявленні та блокуванні шкідливих запитів. Це дозволяє підвищити безпеку та запобігти ефективності цих загроз.

З цієї причини важливо, щоб компанія зосереджувалася на кібербезпеці на запобіганні, а не на вирішенні проблем. Таким чином кіберзагрози не будуть ефективними та не зможуть спричинити проблеми.

Навчання з боротьби з фішингом є одним із найважливіших підходів для компаній, які хочуть уникнути проблем, спричинених цією загрозою. Дозволяючи встановлення шкідливого програмного забезпечення, перенаправляючи конфіденційну інформацію та навіть завдаючи шкоди вашим бізнес-пристроям, проти фішингових атак потрібно боротися за допомогою багатогранного підходу.

Це означає, що окрім використання засобів безпеки, спрямованих на блокування такого типу кіберзагроз, необхідно налагодити процес навчання співробітників, щоб забезпечити додатковий рівень захисту від фішингових атак. Впровадження культури обізнаності про кібербезпеку допоможе користувачам уникнути проблем і зміцнить стратегію захисту, яку використовує ваша

організація.

Стратегії забезпечення стійкості: резервне копіювання та взаємодія з постачальниками DNS. Дуже важливо створювати резервні копії зон DNS. Навіть якщо корпоративний DNS передано постачальнику послуг, яким керує GTI, також потрібно прийняти стратегію резервного копіювання.

Нам потрібно пам’ятати, що незалежно від сектора, в якому вони працюють, компанії вразливі до кібератак, тому важливо використовувати ресурси та методології, щоб уникнути кібератак усіх типів. Прикладом цього була атака на постачальників послуг DNS DYN і Deutshe Telecom [4].

Гіганти в секторі інтернет-послуг, DNS-компанії DYN і Deutshe Telecom зазнали масових DDoS-атак, які надовго порушили їхні послуги та ресурси, залишивши понад 1 мільйон людей без Інтернету. З цієї причини необхідно підготуватися до будь-якого типу інциденту та забезпечити безперервність вашої діяльності незалежно від зазнаної атаки.

1.3. Аналіз існуючих рішень для захисту корпоративної інфраструктури DNS

Система доменних імен (DNS) є основоположним компонентом Інтернету. DNS перетворює зрозумілі людині доменні імена, як-от www.example.com, у машиночитані адреси Інтернет-протоколу (IP), як-от 168.192.123.145. DNS дозволяє користувачам отримувати доступ до веб-сайтів, використовуючи знайомі імена, а не довгі рядки цифр [5, 6].

Незважаючи на свою критичність, інфраструктура DNS спочатку не була розроблена, щоб протистояти багатьом типам кіберзагроз, які хакери використовують, щоб отримати доступ до IT-систем або порушити IT-операції. Безпека DNS це завдання впровадження заходів безпеки та протоколів для пом’якшення вразливостей у системі доменних імен.

Протокол DNS часто називають «телефонною книгою Інтернету», оскільки він збігає назву веб-сайту (ім’я домену) з рядком цифр (IP-адреса), що дозволяє

комп'ютерам швидко знаходити правильну адресу веб-сайт. Ім'я та IP-адреса кожного веб-сайту зберігаються на авторитетному сервері імен десь у світі. Щоб пришвидшити підключення та запобігти перевантаженням на авторитетних серверах, система DNS також використовує рекурсивні DNS-сервери або DNS-перетворювачі, які зазвичай надаються постачальниками послуг Інтернету (ISP). Коли користувач вводить назву веб-сайту в браузері, пристрій користувача спочатку зв'язується з сусіднім рекурсивним DNS-сервером, щоб запитати IP-адресу веб-сайту.

Оскільки рекурсивні DNS-сервери зберігають кеш IP-адрес для багатьох часто використовуваних веб-сайтів, вони часто можуть відповідати на запити DNS, надаючи правильну адресу миттєво. Якщо рекурсивний сервер не має поточної адреси, він зв'яжеться з іншими рекурсивними DNS-серверами або зрештою зв'яжеться з авторитетним сервером імен для точного запису DNS. Цей процес зазвичай відбувається дуже швидко, тому більшість користувачів не знають про процес DNS [5].

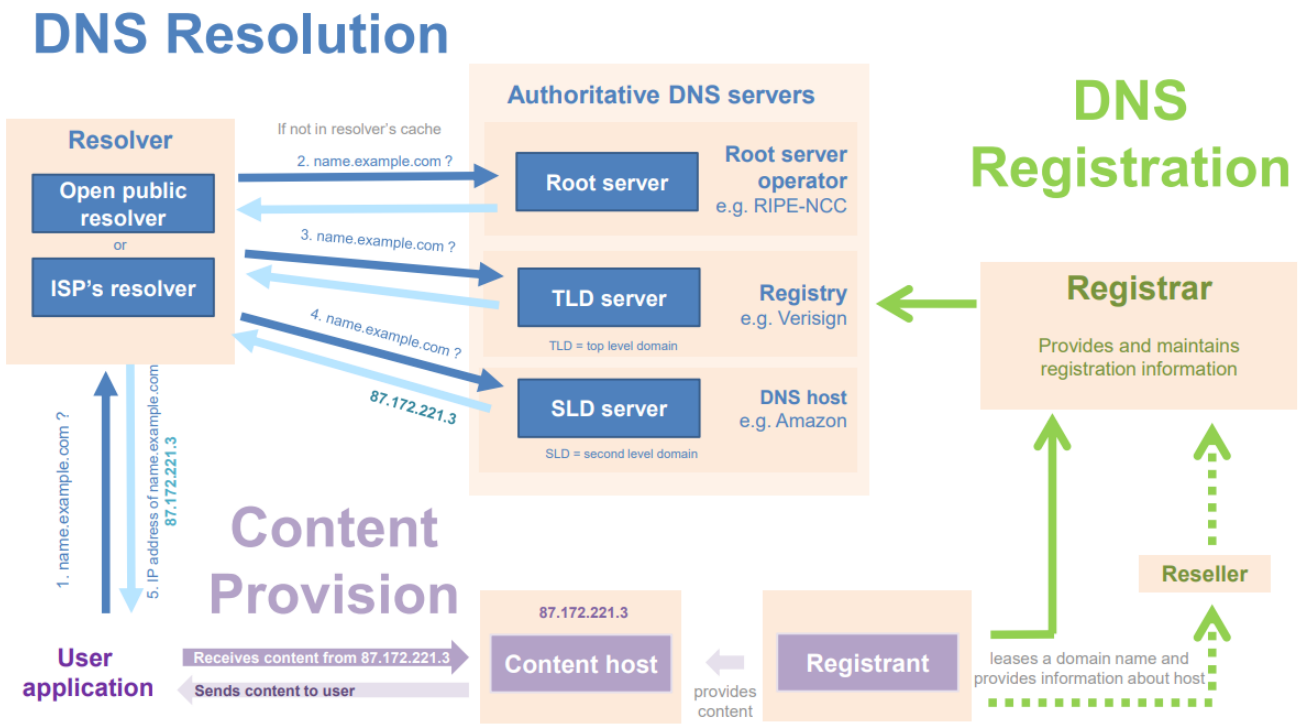

Рис. 1.6. Схема функціонування DNS [6]

Однак DNS вразливий до багатьох кіберзагроз, які можуть перервати відповіді DNS і призвести до збою чи уповільнення роботи серверів, що призведе до повільного завантаження сторінок або неможливості доступу до сайтів в Інтернеті.

Під час реалізації цієї технології діють два важливі процеси, які забезпечують функціонування DNS (рисунок 1.6).

Процес реєстрації, який дозволяє реєстранту здавати в оренду доменне ім'я, тобто придбати ексклюзивне право користування доменним ім'ям на визначений період, зазвичай один рік. Цей процес зазвичай включає реєстранта, реєстр і реєстратора. Його можна описати як «сторону постачання» екосистеми DNS (тобто стосовно особи чи організації, яка надає послуги або контент, наприклад, через веб-сайт, пов'язаний з доменним іменем).

Процес вирішення, який дозволяє програмі користувача отримувати доступ до послуг або вмісту за допомогою вирішення DNS. Цей процес, як правило, включає програму користувача (або «клієнта», на відміну від «сервера»), резолвер і авторитетні сервери DNS (включаючи кореневі сервери, реєстри або сервери верхнього рівня, сервери другого рівня тощо). Його можна описати як «сторону попиту» екосистеми DNS (тобто щодо програми користувача, яка має намір отримати доступ до послуг або вмісту). Як показано на рисунку 1.6, щоб перетворити доменне ім'я на IP-адресу, розпізнавач може:

використовувати вже кешовану інформацію (тобто збережену в базі даних резолвера, як правило, протягом короткого періоду, який називається Time-to-Live або TTL): якщо нещодавно було надіслано запит на те саме ім'я домену, резолвер уже має IP-адресу, що відповідає імені домену;

ініціювати DNS-запит, починаючи з верхньої частини ієрархічної архітектури простору імен DNS (або праворуч від імені домену, як воно відображається в браузері), з кореня, аж до домену верхнього рівня (TLD), другий-домен рівня (SLD) і нижче, де це доречно (наприклад, домени третього рівня). Якщо відповіді на ці пошукові запити вже кешуються розв'язувачем, для прискорення процесу використовується локально кешована інформація.

Важливо, що екосистема DNS належить до логічного рівня, який існує та працює незалежно від веб-сайтів або служб, які надають вміст. Щоб уможливити функціонування цих двох процесів, простір імен DNS структуровано в ієрархічний спосіб, який можна відобразити в розподілену базу даних, покладаючись на різні керовані області або «зони». Коренева зона знаходиться на самому верху цієї ієрархії, як показано на рисунку 1.7. Нижче кореня знаходяться домени верхнього рівня, або TLD, якими керують реєстри. Нижче розташовані реєстри доменів другого рівня, або SLD. У доменному імені, яке відображається у браузері (наприклад, «amazon.co.uk»), ієрархія починається праворуч із кореня, за яким йдуть TLD, SLD та нижчі рівні.

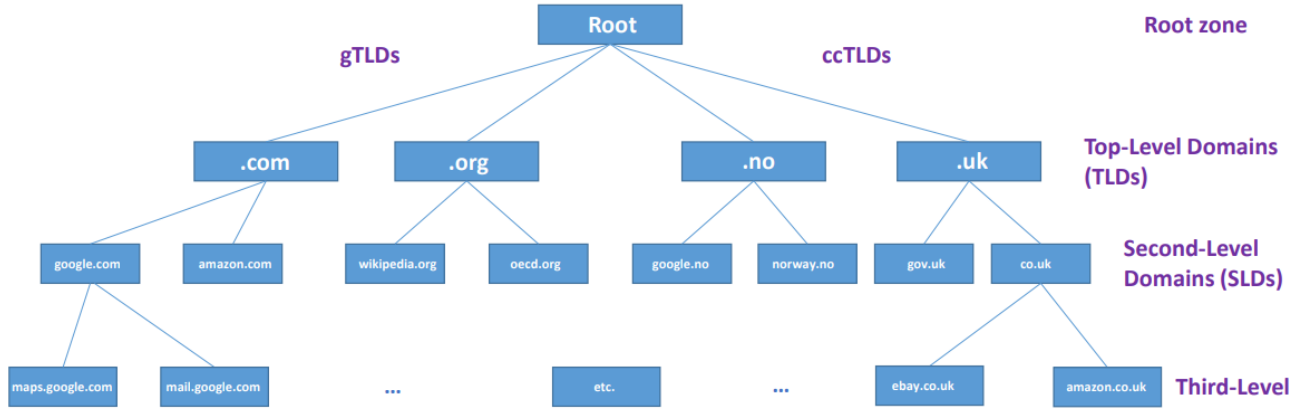

Рис.1.7. Ієрархічна структура простору імен DNS [6]

В [6] зазначається, що не існує узгодженого на міжнародному рівні визначення того, що саме охоплює безпека DNS. Часто виникає плутанина між безпекою DNS і зловживанням DNS, і ці дві категорії іноді можуть збігатися.

Безпека DNS стосується інцидентів, які впливають на доступність, цілісність або конфіденційність частин екосистеми DNS.

Зловживання DNS це ширша категорія, яка включає будь-яке використання DNS зі зловмисною метою, не обов'язково спричиняючи технічний вплив на сам DNS.

Безпека DNS визначається як конкретна сфера цифрової безпеки, яка охоплює інциденти, що порушують доступність, цілісність і конфіденційність

(«тріада AIC») частин екосистеми DNS. Ці інциденти можуть вплинути на будь-якого учасника DNS, а також на будь-які відносини між учасниками DNS (рисунок 1.6) за допомогою одного або кількох із наведених нижче параметрів:

доступність: частина екосистеми DNS недоступна та не може використовуватися за запитом авторизованих користувачів (наприклад, авторитетний сервер другого рівня більше не може надавати відповіді на запит DNS через атаку DNS-затоплення;

цілісність: частину екосистеми DNS було змінено несанкціонованим чином (наприклад, доменне ім’я організації більше не вказує на правильну IP-адресу через атаку викрадення DNS);

конфіденційність: до частини екосистеми DNS отримали доступ неавторизовані організації (наприклад, незашифровані DNS-запити можуть перевірятися третіми сторонами, що може негативно вплинути на конфіденційність користувачів.

Зловживання DNS може охоплювати дві категорії [6]:

використання DNS в атаках на цифрову безпеку, впливаючи на тріаду AIC користувачів Інтернету, без жодного впливу на сам DNS. Доменні імена зазвичай є невід’ємною частиною фішингових кампаній і можуть використовуватися зловмисним програмним забезпеченням або для платформ керування (C2 або C&C) ботнетів, тобто наборів інструментів, які зловмисники використовують для зв’язку зі зламаними пристроями. DNS також можна використовувати як «прихований канал», щоб дозволити зловмисному трафіку непомітно проходити через «тунелювання DNS», яке також може використовуватися для викрадання даних. Цю категорію часто називають «технічним зловживанням» DNS і може вважатися таким, що перекриває безпеку DNS;

використання DNS для незаконної діяльності, окрім атак на цифрову безпеку, тобто без будь-якого впливу на технічному рівні на тріаду AIC користувачів Інтернету або частини DNS, включаючи використання доменних імен для надання доступу до незаконного вмісту (наприклад, порушення авторських прав, ворожнеча, насильство та екстремістський контент тощо). Цю категорію часто

називають DNS «зловживання вмістом».

Одним із провідних рішень у сфері безпеки DNS є Heimdal [2]. Heimdal забезпечує комплексний захист DNS із такими функціями, як виявлення та блокування загроз у реальному часі, фільтрація DNS і безпечне вирішення DNS.

Рішення Heimdal призначені для захисту від широкого спектру атак на основі DNS і підвищення загальної безпеки мережі.

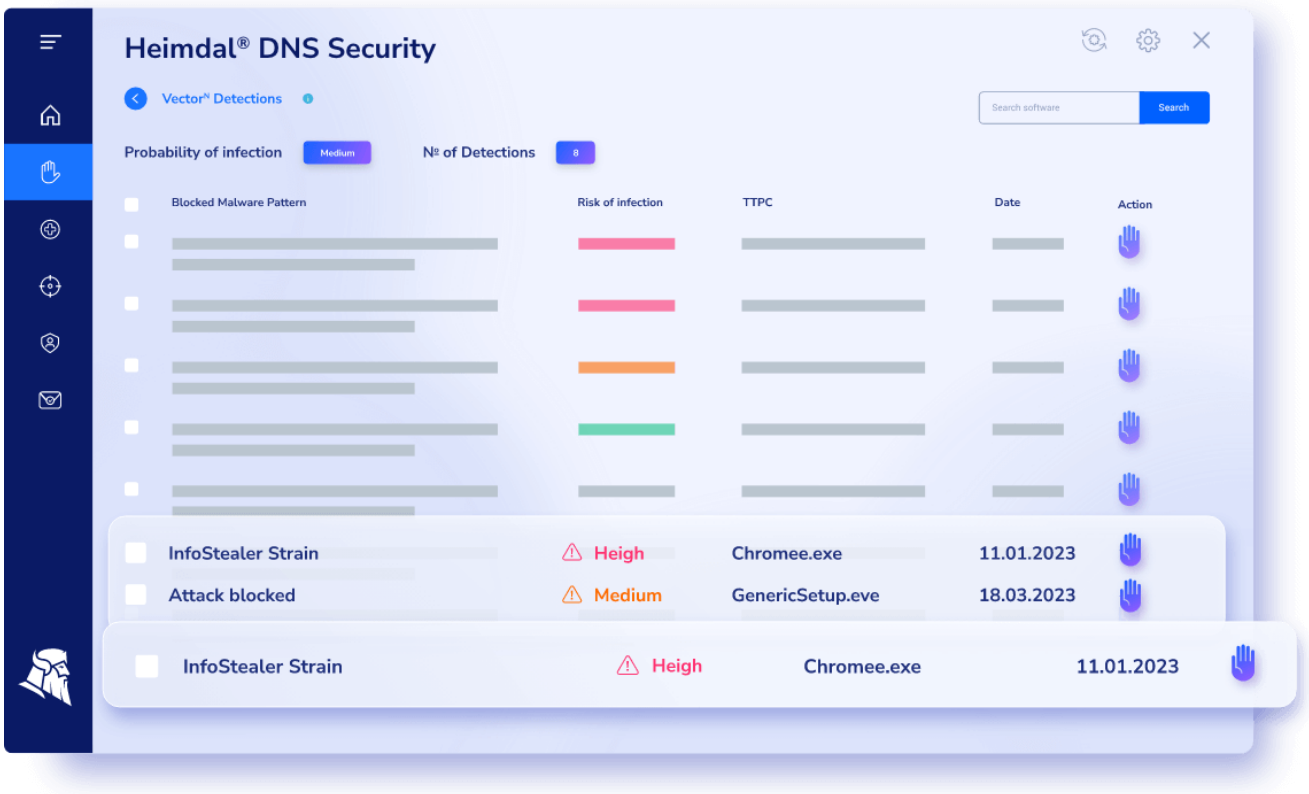

Рис. 1.8. Інтерфейс рішення Heimdal [2]

Рішення Heimdal забезпечує безпеку DNS такими способами [2]:

DNS Security від Heimdal використовує механізм DarkLayer Guard для фільтрації трафіку DNS. Цей механізм створює локальний DNS-сервер, який перевіряє пакети даних перед вирішенням DNS-запитів. Якщо під час запиту виявляється будь-яка підозріла активність, з'єднання автоматично блокується. Ця проактивна фільтрація запобігає потраплянню шкідливих даних на ваші кінцеві точки та мережу;

VectorN Detection покращує безпеку, визначаючи шаблони в блоках домену

за допомогою вдосконалених алгоритмів машинного навчання. Він може виявляти навіть шкідливі програми, аналізуючи поведінку заблокованих доменів. У разі виявлення шкідливих шаблонів система позначає потенційно заражені кінцеві точки для подальшого дослідження. Це включає розпізнавання незвичайної частоти блокування домену, що може вказувати на наявність розвинутих постійних загроз або ботнетів;

DNS Security від Heimdal працює на рівнях DNS, HTTP і HTTPS, забезпечуючи комплексний захист. Маршрутизуючи весь інтернет-трафік через локально налаштовану базу даних, Heimdal може ідентифікувати та блокувати доступ до відомих шкідливих веб-сайтів;

Heimdal інтегрував DNS через HTTPs (DoH) у своє рішення безпеки. DoH шифрує трафік DNS, знижуючи ризик підробки DNS і атак типу Man-in-the-middle (MitM). Це шифрування забезпечує безпечний і приватний досвід перегляду без шкоди для продуктивності системи, що зрештою економить час і ресурси для організацій. Пакет засобів захисту DNS від Heimdal розроблений для бездоганної роботи з будь-якою існуючою інфраструктурою безпеки. Доступний як на рівні кінцевої точки, так і на рівні мережі, його можна швидко розгорнути та добре інтегрується з іншими засобами безпеки, такими як брандмауери та антивірусне програмне забезпечення. Ця сумісність дозволяє організаціям підвищити рівень безпеки з мінімальними збоями;

Окрім цих п’яти основних функцій захисту, рішення безпеки DNS Heimdal також [2]:

виявляє спроби викрадення DNS;

ідентифікує процеси, користувачів, URL-адреси та походження зловмисників, які беруть участь у проникненні в мережу;

прогнозує майбутні загрози DNS із точністю 96% за допомогою ШІ;

пропонує блокування на основі категорії для кінцевих рішень;

всебічно реєструє мережевий трафік для кращої видимості та керування.

Отже, безпека DNS передбачає захист інфраструктури DNS від кіберзагроз для забезпечення її швидкої та надійної роботи. Надійна стратегія безпеки DNS

включає кілька рівнів захисту, наприклад розгортання резервних DNS-серверів, впровадження протоколів безпеки, таких як DNSSEC, і забезпечення ретельного журналювання DNS.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ КОРПОРАТИВНОЇ ІНФРАСТРУКТУРИ DNS НА БАЗІ AKAMAI EDGE DNS

2.1. Призначення та основні функції рішення Akamai Edge DNS

Сервери системи доменних імен (Domain Name System, DNS) перетворюють доступні для читання імена хостів доменів, як-от *www.companywebsite.com*, на IP-адреси, які можуть читати машини. DNS-сервери мають важливе значення для забезпечення позитивного досвіду перегляду, а також для швидкого й надійного інтернет-з'єднання з веб-сайтами, API та програмним забезпеченням корпоративних додатків, розміщених у хмарі [11].

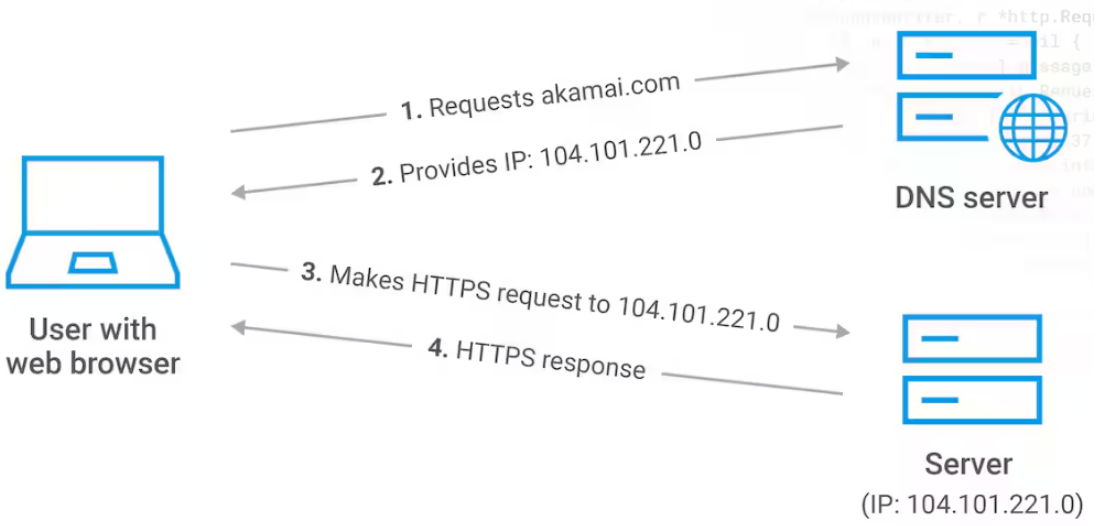

Рис. 2.1. Принцип роботи DNS-сервера [11]

Існують чисельні загрози для DNS-серверів у вигляді будь-яких типів атак, які ставлять під загрозу доступність, швидкість і продуктивність служб DNS. До них належать DNS-флуд, які переповнюють DNS-сервери запитами на ресурси, що робить сервери недоступними для законних запитів. Підробка DNS або отруєння кешу – це тип кібератаки, яка перенаправляє трафік на шахрайський веб-сайт. DNS-тунелювання використовує дані, закодовані в DNS-запитах і відповідях, щоб захопити DNS-сервер і дозволити зловмисникам керувати ним віддалено.

Тому, захист DNS-серверів є критично важливим бізнес-пріоритетом для команд безпеки організацій. Оскільки DNS дозволяє корпоративним користувачам отримувати доступ до веб-додатків і API організації, будь-яка загроза корпоративним DNS-серверам також є загрозою бізнес-операціям, прибутковості та довірі клієнтів і партнерів [11].

Продукт Akamai Edge DNS – це хмарне рішення, яке забезпечує доступність 24/7, покращує швидкість реагування та покращує стійкість DNS-серверів, оскільки вони захищаються від найбільших DDoS-атак.

Akamai Edge DNS – це авторитетна служба DNS. Це рішення забезпечує безпечну, високопродуктивну, масштабовану та високодоступну крайову службу для авторитетного DNS. Akamai Edge DNS використовує глобальне розгортання Akamai тисяч серверів імен у кількох мережах, використовує IP Anycast і покладається на власну реалізацію протоколу DNS як загального компонента Akamai Intelligent Platform.

Рішення Akamai Edge DNS доповнює існуючі веб-інфраструктури, незалежно від того, розгортаються вони в приватному центрі обробки даних чи публічній хмарі, з’єднуючи користувачів із бажаним пунктом призначення.

Akamai Edge DNS використовує модель IP anycast для відповіді на запити DNS. Це означає, що замість того, щоб покладатися на два чи три DNS-сервери, клієнти Akamai можуть отримати доступ до тисяч серверів імен, розгорнутих у більш ніж 4100 точках присутності по всьому світу. IP anycast спрямовує запити від кінцевих користувачів до найближчої точки присутності для вирішення, забезпечуючи швидшу продуктивність, більший масштаб і більш різноманітний розподіл. Хоча використання IP anycast не є унікальним для Akamai, ми також сегментуємо сервери імен і точки присутності в кілька хмар IP anycast, роблячи Edge DNS еквівалентним кільком автономним постачальникам DNS з точки зору доступності, масштабу та розподілу. На рисунку 2.2 показано схему реалізації технології Akamai Edge DNS [12].

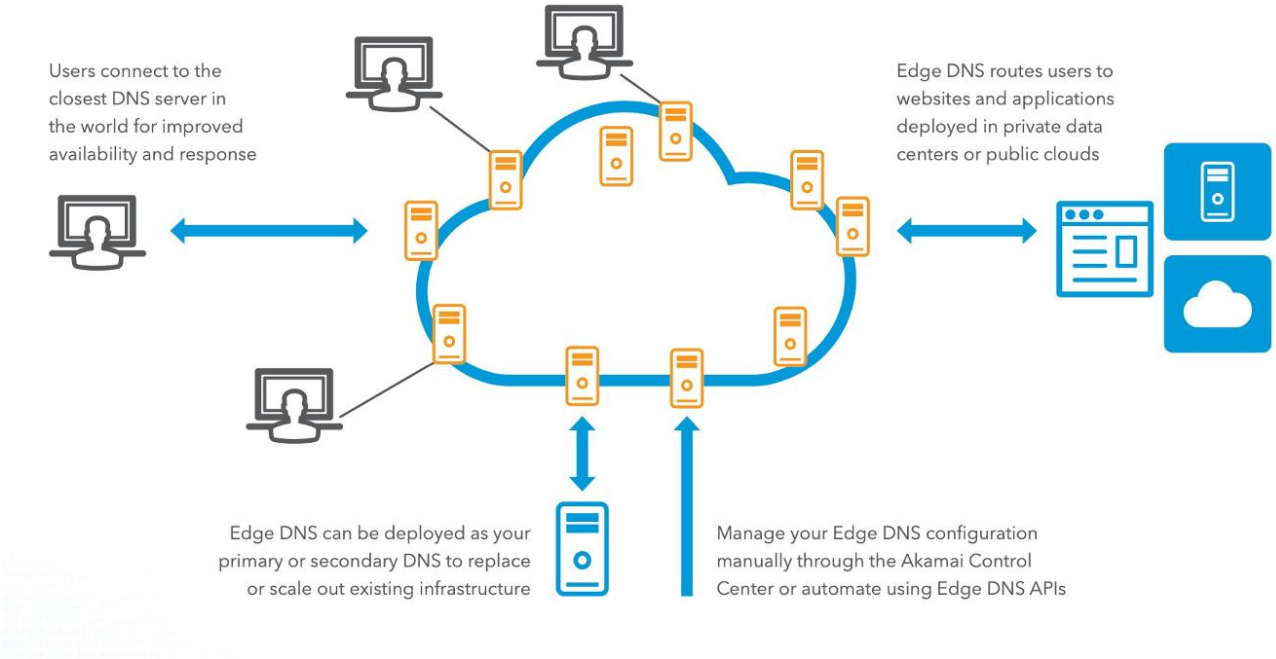

Рис. 2.2. Схема реалізації технології Akamai Edge DNS [3]

Функції рішення Akamai Edge DNS включають наступне [12]:

запатентована реалізація протоколу DNS, яка використовує всесвітню інфраструктуру DNS Akamai;

підтримка первинної та вторинної зон;

DNSSEC, якщо Akamai Edge DNS придбано з опцією безпеки;

Zone apex mapping, що скорочує час пошуку DNS для веб-сайтів на інтелектуальній платформі;

псевдоніми зон, які базуються на ресурсних записах іншої зони Akamai Edge DNS;

підтримка серверів персональних імен, які можуть вказувати на IP-адреси Akamai Edge DNS Anycast. IP Anycast надає кінцевим користувачам децентралізовану службу DNS. За допомогою IP Anycast можна створити логічний сервер імен, який складається з кількох фізичних серверів імен, розгорнутих у кількох мережах і на різних континентах;

API для програмного доступу до звітних даних і керування зонами;

служби доставки журналів для доступу до журналів транзакцій;

забезпечення вимог відповідно RFC 1034 і 1035.

Необхідно відмітити, що IP anycast – це техніка мережевої маршрутизації, при якій кілька ідентичних мережевих вузлів розгортаються в розподіленій мережі для надання єдиної спільної IP-адреси. Усі вузли відповідають на ту саму IP-адресу, а трафік направляється до найближчого вузла на основі протоколів маршрутизації, що забезпечує користувачам найнижчу затримку та найвищу доступність.

Ролі, які найчастіше відповідають за керування Akamai Edge DNS, це адміністратори сайту, менеджери проектів і постачальники технічної підтримки.

Отже, Akamai Edge DNS надає хмарне DNS-рішення, яке допомагає організаціям підвищити доступність, продуктивність і відмовостійкість розв'язання DNS і покращити взаємодію з користувачами для своїх веб-сайтів і додатків. Рішення Akamai Edge DNS доповнює існуючі веб-інфраструктури, незалежно від того, розгортаються вони в приватному центрі обробки даних чи публічній хмарі, швидко й ефективно з'єднуючи користувачів із бажаним пунктом призначення.

Рішення Akamai Edge DNS використовує глобальну мережу DNS Akamai, яка включає тисячі серверів імен, розгорнутих у сотнях точок присутності (PoP) у понад 40 країнах. У будь-якому регіоні точки присутності Akamai розподіляються між кількома мережами для резервування та охоплення як на географічному, так і на мережевому рівнях.

2.2. Порядок реалізації основних функцій рішення Akamai Edge DNS

Akamai Edge DNS надає хмарне DNS-рішення, яке допомагає організаціям підвищити доступність, продуктивність і відмовостійкість розв'язання DNS і покращити взаємодію з користувачами для своїх веб-сайтів і додатків. Akamai Edge DNS доповнює існуючі веб-інфраструктури, незалежно від того, розгортаються вони в приватному центрі обробки даних чи публічній хмарі, швидко й ефективно з'єднуючи користувачів із бажаним пунктом призначення [12].

Розгортання Akamai Edge DNS глобально поширюється в кількох мережах. Edge DNS використовує глобальну мережу DNS Akamai, що включає тисячі

серверів імен, розгорнутих у сотнях точок присутності (PoP) у понад 40 країнах. У будь-якому регіоні точки присутності Akamai розподіляються між кількома мережами для резервування та охоплення як на географічному, так і на мережевому рівнях [12].

Реалізується IP Anycast. Edge DNS покладається на технологію IP Anycast для надання децентралізованої служби DNS кінцевим користувачам. За допомогою IP Anycast організації можуть створити логічний сервер імен, який складається з кількох фізичних серверів імен, розгорнутих у кількох мережах і на різних континентах.

Власна реалізація DNS. Edge DNS не запускає програмне забезпечення на основі Berkeley Internet Name Domain (BIND). Натомість він покладається на запатентовану реалізацію протоколу DNS, яка використовує великий власний досвід Akamai у розробці, управлінні та моніторингу всесвітньої інфраструктури DNS. Це захищає рішення Edge DNS від зловмисників, які намагаються використати різні вразливості безпеки, які були виявлені в BIND.

Сервери імен Akamai сумісні з RFC 1034 і 1035, а також багатьма наступними.

Первинна, вторинна та псевдонімні зони.

Зона DNS – це окрема частина або адміністративний простір у просторі імен домену DNS, який розміщено на сервері DNS. Зони DNS дозволяють розділити простір імен DNS для адміністрування та резервування. DNS-сервер може бути авторитетним для кількох зон DNS.

Уся інформація про зону зберігається у файлі, який містить записи бази даних DNS для всіх імен у цій зоні. Ці записи містять зіставлення між IP-адресою та іменем DNS. Файли зон DNS завжди мають починатися із запису Start of Authority (SOA), який містить важливу адміністративну інформацію про цю зону та про інші записи DNS.

Ми можемо розгорнути рішення Akamai Edge DNS як основний або вторинний DNS, замінивши або розширивши існуючу інфраструктуру DNS за бажанням. Незалежно від того, основний чи вторинний, Edge DNS може надати

організації масштабовану та захищену мережу DNS, яка допомагає забезпечити найкращий досвід для користувачів.

Первинна зона. Коли ми створюємо основну зону, ми надаємо Akamai свої записи DNS для зберігання та керування ними. Ми можемо вносити зміни в ці записи за допомогою інтерфейсу користувача Control Center або Edge DNS Zone Management API. Akamai надсилає дані зон на сервери імен Edge DNS і надає список серверів імен, які можна зареєструвати у реєстратора домену.

Вторинна зона. Коли ми створюємо вторинну зону, ми підтримуємо авторитетну версію своїх записів DNS на головних серверах імен. Агенти передачі зони (ZTA) надсилають дані зони на сервери імен Edge DNS.

Крім того, підтримуються *псевдоніми зон*. За допомогою псевдонімних зон Akamai автоматично віддзеркалює конфігурацію іншої крайової DNS- зони, обслуговуючи ті самі записи DNS як у зоні псевдонімів, так і в цільовій зоні. Наприклад, можливо, ми зареєстрували домен з орфографічною помилкою, як-от, і хочемо, щоб він мав ті самі записи DNS, що й *.examlpe.comexample.com*

Агенти перенесення зон (Zone transfer agents, ZTA)

ZTA надсилають дані зони з корпоративних головних серверів імен на сервери імен Edge DNS. ZTA використовуються лише для передачі даних для вторинних зон.

ZTA відповідають стандартним протоколам, описаним у RFC 1034 і 1035, і працюють із найпоширенішими первинними серверами імен, включаючи BIND (версія 9 і пізніші), Microsoft Windows Server і Microsoft DNS Consortium від Internet Systems Consortium.

Інтервали оновлення та повторних спроб у записі початку повноважень (Start of authority, SOA) визначають інтервал між передачами зон. Крім того, ми можемо налаштувати систему на прийом запитів NOTIFY від наших вторинних зон, щоб дозволити майже негайне оновлення.

ZTA розгортаються в надлишковій конфігурації в кількох фізичних і мережевих розташуваннях по всій мережі Akamai. Усі ZTA намагатимуться виконати передачу зони з корпоративного головного сервера імен, але лише одна

ZTA (зазвичай перша, яка отримує оновлення за допомогою однієї передачі) надсилатиме оновлення зони на сервери імен. У цьому процесі використовується власна відмовостійка інфраструктура передачі даних, що забезпечує відмовостійку систему на кожному рівні.

Делегування підзони між обліковими записами

Делегування підзон між обліковими записами надає власнику батьківської зони механізм безпечного надання іншому обліковому запису Edge DNS можливості делегувати підзони в існуючих зонах власника. Власник зони, який бере участь у запитах на надання підзони, повинен мати свій договір Edge DNS, авторизований для надання підзони. При цьому необхідно звернутися до представника сервісної служби для авторизації.

Після того як представник служби додасть договір власника зони до списку дозволених, власник зони може ввімкнути делегування підзони для вказаної зони. Увімкнення створення підзони дозволяє будь-якому клієнту Akamai подати запит на підзону для цієї зони.

Без схваленого запиту на надання підзони кожна підзона починає перебувати в стані PENDING_APPROVAL. Власник підзони може почати створювати записи та завантажувати файли зони, поки він очікує схвалення свого запиту від власника зони. Власник зони отримує сповіщення про будь-які запити підзони, що очікують на розгляд, і схвалює або відхиляє їх під час процесу перегляду.

Вихідні зональні трансфери

Передача вихідної зони дозволяє передавати дані зони з межових DNS-серверів на зовнішні сервери імен. Це корисно, якщо організація використовує кілька постачальників послуг для DNS і нам потрібно підтримувати головний файл зони з даними зони. Авторитетні передачі зон (AXFR) використовуються для передачі даних зон на наші зовнішні сервери імен.

Ми можемо ввімкнути передачу вихідної зони під час створення або зміни основної чи додаткової зони. У рамках цієї конфігурації ми надаємо таку інформацію [12]:

цілі сповіщень: IP-адреси серверів імен, з якими здійснюється зв’язок, коли

дані зони доступні для передачі. Коли з’являється нова версія файлу зони, Akamai надсилає запит NOTIFY кожному цільовому серверу або серверу імен, який ви налаштовуєте. Запит NOTIFY – це сповіщення, яке вказує на наявність нових даних. Цей запит зазвичай ініціює передачу зони;

список контролю доступу: список IP-адрес або блоків CIDR, які використовуються для передачі зони. Ці адреси є єдиними, за якими дозволено передавати дані з межових DNS-серверів на наш зовнішній сервер імен. Цілі сповіщень автоматично включаються до списку керування доступом (ACL). Однак ми можемо пропустити їх зі списку;

ключ передачі підпису (TSIG). Цей ключ використовується для захисту обміну повідомленнями DNS для передачі зон. Ми можемо вибрати наявний ключ або створити новий ключ.

Картування вершини зони

Відображення вершини зони використовує дані відображення, доступні на платформі Akamai, щоб скоротити час пошуку DNS для корпоративних веб-сайтів.

Завдяки відображенню верхівки зони сервери імен вирішують запити на пошук DNS за допомогою IP-адреси оптимального периферійного сервера.

DNSSEC для Edge DNS

Розширення безпеки DNS (DNSSEC), описані в RFC 4033, 4034 і 4035, дозволяють адміністраторам зон підписувати цифровим підписом дані зони за допомогою криптографії з відкритим ключем, підтверджуючи їх автентичність. Основна ідея DNSSEC полягає в запобіганні отруєнню кешу DNS і викраденню DNS. Ці типи записів використовуються для DNSSEC [12]:

DNSKEY (відкритий ключ DNS). Зберігає відкритий ключ, який використовується для підписів наборів записів ресурсів;

RRSIG (підпис запису ресурсу). Зберігає підпис для набору ресурсних записів (RRset);

DS (підписант делегації). Покажчик батьківської зони на DNSKEY дочірньої зони;

NSEC3 (наступний безпечний v3). Використовується для автентифікованого

NXDOMAIN.

Елемент контракту Security Option Edge DNS підтримує такі функції [12]:

підпис і обслуговування DNSSEC. Akamai керує підписом зони, ротацією ключів і обслуговуванням зони;

служба DNSSEC. Ми керуємо підписом зони та ротацією ключів, а Akamai обслуговує зону.

Функція DNSSEC Sign and Serve надає можливість повністю розвантажити підтримку DNSSEC на існуючу інфраструктуру керування ключами Akamai (KMI) для ротації ключа підпису зони (ZSK) і ключа підпису ключа (KSK).

ZSK змінюється щотижня, а KSK – щорічно. Для ротації ключів зони Akamai використовує метод RFC 4641, модифікований для постійної ротації. Тобто в записі DNSKEY вершини зони присутні два ZSK. Один ключ активно підписує решту зони, тоді як інший ключ присутній, тому він має час для поширення, перш ніж стати активним. Цей метод:

додає новий запис DNSKEY, який ще не використовувався, у верхівку DNSKEY RRset;

очікує на поширення даних (час поширення плюс TTL набору ключів);

перемикається на підписання RRSIG зони новим ключем, але залишає попередній ключ доступним у верхньому DNSKEY RRset;

очікує час поширення плюс максимальний TTL у зоні;

видаляє старий ключ із вершини DNSKEY RRset, який потім перезапускає процес ротації ключів.

Термін підписання – три дні. Щоб гарантувати, що термін дії підписів не закінчиться, навіть якщо записи не змінюються, зона повторно підписується принаймні раз на день.

Додатковою перевагою DNSSEC Sign and Serve є можливість підтримувати перенаправлення верхнього рівня. Поточний рекомендований алгоритм ECDSA-P256-SHA256 або RSA SHA-256, якщо ми хочемо уникнути використання ECDSA.

DNSSEC можна використовувати як із ZAM, так і з перенаправленням верхнього рівня.

Служба DNSSEC

Функція обслуговування DNSSEC надає можливість підтримувати DNSSEC для вторинних зон, але адміністратор зони несе відповідальність за впровадження власного рішення інфраструктури керування ключами (KMI) і правильну ротацію ключа підпису зони (ZSK) і ключа підпису ключа (KSK).

Для DNSSEC потрібен підпис транзакції (TSIG). Для контролю доступу до зони потрібно ввімкнути TSIG за допомогою підтримуваних алгоритмів. Окрім нашої відповідальності за підписання всіх ключів, ми маємо переконатися, що всі необхідні нові записи знаходяться в зоні передачі до Akamai.

Псевдонім зони – це тип зони, який не має власного файлу зони. Натомість він базується на записах ресурсів (основної чи вторинної) іншої (основної) зони Edge DNS (базової). Іншими словами, дані зони є копією іншої зони Edge DNS. Ми можемо змінювати дані в зонах псевдонімів, змінюючи «батьківську» зону або зону «псевдонім».

Організація може мати кілька сотень брендових доменів або доменів, які потрібно зареєструвати та для яких потрібні служби DNS, але для яких DNS налаштовано так само, як і базова зона. У цих випадках ми можемо налаштувати одну базову зону, вказати багато псевдонімів на базову зону та легко керувати будь-якими змінами DNS, оновлюючи лише файл базової зони.

За замовчуванням контракти Edge DNS обмежені 2000 налаштованими зонами, включаючи псевдоніми. Псевдоніми зон генерують власні рядки журналу незалежно від базової зони. Щоб отримувати журнали з трафіком зони псевдонімів, потрібно ввімкнути доставку журналів для кожної зони псевдонімів окремо.

Зони псевдонімів сумісні з:

картування вершини зони;

CNAME верхнього рівня (може налаштувати лише служба технічної підтримки);

сервери персональних імен (ці записи серверів імен не мають бути з базової зони з псевдонімами).

Зони псевдонімів несумісні з DNSSEC. Для кожної зони DNSSEC потрібні

власні підписи записів ресурсів. Базові зони з увімкненою DNSSEC не можуть мати жодних псевдонімів.

Приклад зони псевдонімів

Цей приклад відображається у стандартному форматі зони BIND.

Таблиця 2.1

Базова зона example-base-zone.com має такі записи ресурсів

Zone name	TTL	Record class	Record type	Record data
www.example-base-zone.com	7200	IN	A	192.0.2.1
www.example-base-zone.com	7200	IN	AAAA	::1
store.example-base-zone.com	7200	IN	CNAME	store.example-base-zone.com.edgesuite.net.

Зона налаштована як псевдонім. Кожного разу, коли запит DNS запитує дозвіл запису ресурсу в зоні псевдоніма, Edge DNS відповість із записами ресурсів, указаними в базовій зоні *example-alias-zone.com*, як якщо б зона псевдоніма *www.example-base-zone.com* мала ті самі записи ресурсів, що й базова зона (таблиця 2.2).

Таблиця 2.2

Зона налаштована як псевдонім

Zone name	TTL	Record class	Record type	Record data
www.example-alias-zone.com	7200	IN	A	192.0.2.1
www.example-alias-zone.com	7200	IN	AAAA	::1
store.example-alias-zone.com	7200	IN	CNAME	store.example-base-zone.com.edgesuite.net.

Кожного разу, коли вноситься зміна до записів ресурсів базової зони, усі псевдоніми цієї зони відображатимуть ту саму зміну.

2.3. Алгоритм роботи рішення Akamai Edge DNS

Рішення Akamai зменшує ризик DDoS-атак за допомогою швидкого та ефективного захисту, призначеного для протидії найбільшим і найскладнішим DDoS-атакам, незалежно від того, розгортаються додатки в центрі обробки даних, публічній хмарній інфраструктурі чи спільному розміщенні [10].

На рисунку 2.3 показано порядок захисту від DDoS атак платформи Akamai, який складається з наступних кроків [10]:

1. Клієнти виконують DNS-пошук у службі DNS Akamai, яка поглинає навіть найбільші DDoS-атаки.

2. Граничні сервери автоматично перевіряють трафік CDN на наявність атак DDoS, веб-додатків і ботів і блокують зловмисні загрози.

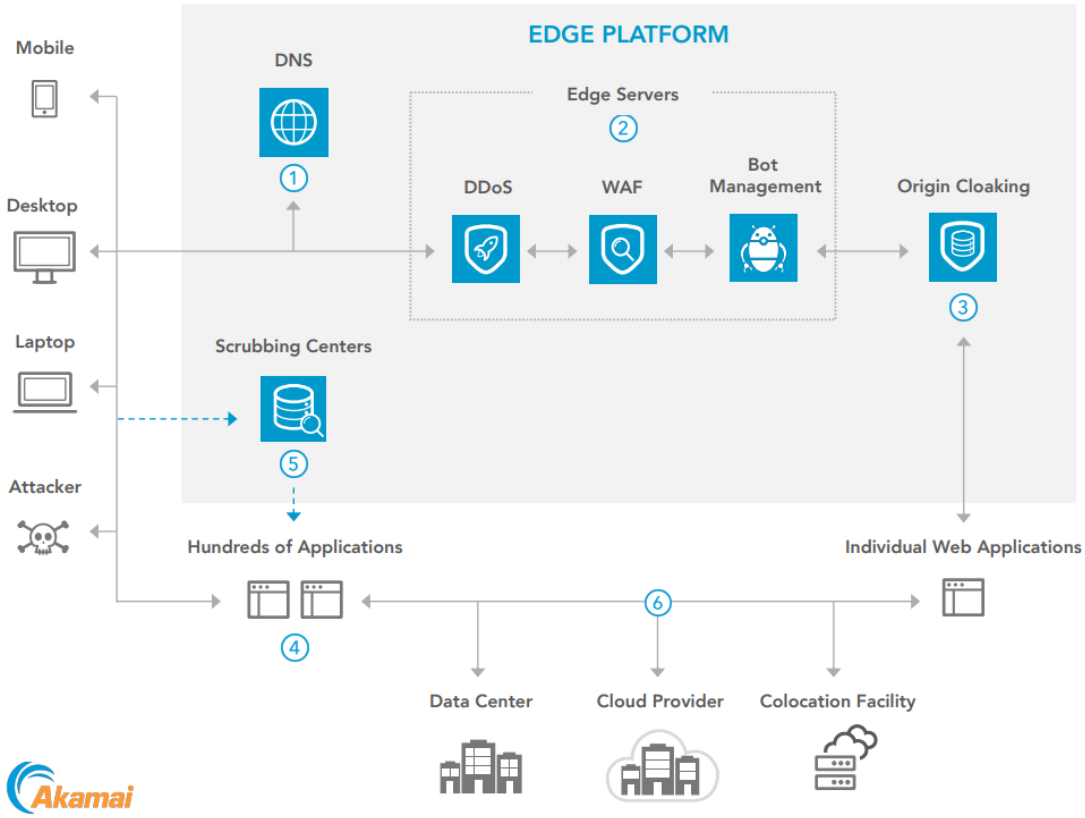

Рис. 2.3. Архітектура захисту від DDoS атак [10]

3. Akamai направляє трафік CDN через призначені периферійні сервери, дозволяючи клієнтам відключати трафік з інших джерел і запобігати зловмисникам в обхід периферійного захисту.

4. Трафік, не пов’язаний із CDN, зазвичай направляється безпосередньо до джерела на основі рекламних оголошень про маршрути BGP клієнта.

5. Клієнти можуть направляти трафік через центри очищення Akamai (завжди ввімкнені або на вимогу), де DDoS-атаки блокуються за допомогою проактивного контролю пом’якшення або активного пом’якшення SOC.

6. Сервіси Akamai на основі CDN і DDoS-скрабінгу можуть захистити програми, розгорнуті в клієнтських центрах обробки даних, загальнодоступній хмарній інфраструктурі або на об’єктах спільного розміщення.

3 ТЕХНОЛОГІЯ ЗАХИСТУ КОРПОРАТИВНОЇ ІНФРАСТРУКТУРИ DNS НА БАЗІ AKAMAI EDGE DNS

3.1. Порядок застосування рішення Akamai Edge DNS

Необхідно відмітити, що *зона DNS* є окремою логічною сутністю у просторі імен домену системи доменних імен (DNS), яка використовується для надання більш детального контролю адміністратору, організації чи іншій юридичній особі, відповідальній за керування нею [14].

Зони DNS розподіляють повноваження над різними сегментами простору імен DNS, наприклад, доменом і субдоменом, що дає адміністраторам більш точний контроль над записами DNS, серверами імен DNS та іншими компонентами. Це розділення може допомогти оптимізувати керування DNS і оркестровку, а також розподілити навантаження між серверами імен.

Наприклад, домен «example.com» може існувати в тій самій зоні, що й субдомени «blog.example.com» і «community.example.com». Якщо адміністраторам потрібен більш детальний контроль (можливо, через кількість пристроїв, підключених до сайту спільноти, і обсяг пов’язаних записів DNS) вони можуть розділити субдомен «community.example.com» на власну зону з власним авторитетним сервером імен.

Зона DNS визначає, що доменом або частиною домену керує певний адміністратор. У той же час зона може охоплювати кілька субдоменів, і в одному можуть існувати кілька зон

DNS сервер. Зони DNS не передбачають фізичного розділення, але використовуються для контролю над різними частинами простору імен.

Зони можуть полегшити адміністративне навантаження, пов’язане з доменом, розподілити навантаження запитів DNS і підвищити загальну ефективність і масштабованість служб DNS. Ефективне керування зонами, яке використовує такі функції безпеки, як DNSSEC і динамічні оновлення, може

посилити безпеку DNS і зменшити загрози безпеці, такі як підробка DNS і атаки викрадення [14].

DNS як ієрархічний децентралізований компонент стандартного Інтернет-протоколу відповідає за перетворення зручних для людини доменних імен на адреси Інтернет-протоколу (IP), які комп'ютери використовують для ідентифікації один одного в мережі. Коли користувач вводить ім'я домену в браузері, починається запит (який часто називають запитом DNS або пошуком DNS). Рекурсивний розпізнавач є посередником між клієнтським пристроєм і авторитетними серверами. Він запитує серію серверів, щоб знайти інформацію, необхідну для підключення користувача до потрібного веб-сайту. Кожен із цих серверів відповідає за сегмент простору доменних імен.

Процес запиту починається з кореневого сервера імен. Кореневі сервери імен розташовані на вершині ієрархії DNS і відповідають за керування кореневою зоною. Ці сервери відповідають на запити щодо записів, що зберігаються в кореневій зоні, і направляють запити на відповідний сервер імен домену верхнього рівня (TLD).

Сервери імен TLD спрямовують запити до авторитетних серверів імен для конкретних доменів у межах їх TLD. Наприклад, сервер імен TLD для «.com» направляє домени, що закінчуються на «.com», сервер імен TLD для «.gov» спрямовує домени, що закінчуються на «.gov» тощо.

Сервер доменних імен (іноді його називають сервером доменних імен другого рівня) містить файл зони з IP-адресою для повного доменного імені, наприклад «ibm.com». Цей файл зони також може містити інформацію для субдомену (наприклад, blog.ibm.com) або ця інформація може бути розділена на власну зону. Кожен із цих серверів зберігає записи DNS з інформацією про домен, який потрібен рекурсивному резолверу для продовження та остаточного вирішення запиту.

Файл зони DNS – це простий текстовий файл, який зберігається на DNS-серверах і містить усі записи для доменів у цій зоні. Кожен рядок файлу зони визначає запис ресурсу (один фрагмент інформації про природу, зазвичай

упорядкований за типом даних). Записи ресурсів гарантують, що коли користувач ініціює запит, DNS може швидко спрямувати користувачів на правильний сервер.

Файли зони DNS починаються з двох обов'язкових записів: початок повноважень (запис SOA), який визначає основний авторитетний сервер імен для зони DNS, і глобальний час життя (TTL), який вказує, як записи повинні зберігатися в локальній системі. Кеш DNS.

Файл зони може містити кілька інших типів записів, зокрема [14]:

записи A, які зіставляються з адресами IPv4, і записи AAAA, які зіставляються з адресами IPv6;

записи обмінника поштою (MX-записи), які визначають сервер електронної пошти SMTP для домену;

записи канонічних імен (записи CNAME), які переспрямовують імена хостів із псевдоніма в інший домен («канонічний домен»);

записи сервера імен (NS-записи), які вказують на те, що сервер DNS приєднаний до певного офіційного сервера імен;

записи покажчиків (записи PTR), які визначають зворотний пошук DNS;

текстові записи (TXT-записи), які вказують на структурний запис політики відправника для автентифікації електронної пошти.

Первинна зона DNS – це основна зона DNS зберігає файл основної зони з усіма записами DNS для цієї зони. Це копія для читання/запису, а оновлення зони вносяться до основної зони, а потім копіюються у вторинні зони. Одночасно на одному DNS-сервері може бути лише одна основна зона.

Вторинна зона DNS є додатковою зоною. Це копія основної зони, доступна лише для читання, яка використовується для створення резервування та реалізації балансування навантаження для запитів DNS.

Запити DNS зазвичай розподіляються між основним і вторинним серверами. Якщо основний сервер не працює, вторинні сервери можуть взяти на себе все або частину навантаження за допомогою передачі зон – транзакції, яка дає змогу первинному та додатковому серверам обмінюватися зонами. Вторинні зони також перевіряються на первинних серверах, щоб переконатися, що репліки актуальні.

Зона прямого огляду. Зона прямого пошуку перетворює доменні імена в IP-адреси. Коли DNS-розпізнавач отримує запит на зрозуміле доменне ім'я, він звертається до записів зіставлення A або AAAA в зоні прямого пошуку, щоб знайти відповідну IP-адресу.

Зона зворотного пошуку – як контрапункт зон прямого пошуку, зони зворотного пошуку відображають IP-адреси назад у доменні імена за допомогою записів PTR (записів-вказівників).

Цей процес може бути корисним для розгортання служб, які потребують перевірки домену, або для цілей реєстрації, коли командам потрібно зрозуміти домен, пов'язаний з IP-адресою (наприклад, усунення несправностей і фільтрація спаму). Запити в зонах зворотного пошуку DNS використовують *in-addr.arpa* або домени *ip6.arpa*.

Зони-заглушки містять лише записи, необхідні системі для ідентифікації повноважних серверів імен для зони. Вони служать покажчиками, зменшуючи залежність від рекурсивних серверів для запитів зон верхнього рівня, щоб знайти авторитетний сервер. Близькість заглушених зон до авторитетних серверів допомагає зменшити трафік DNS-запитів і скоротити час вирішення.

Передача зон DNS підтримує оптимальну функціональність системи, особливо в середовищах, де надлишковість і висока доступність є пріоритетними.

Повна передача зони копіює весь вміст файлу зони з основного DNS- сервера на вторинні сервери, створюючи точну копію зони. Повні передачі зон зазвичай використовуються під час початкової конфігурації вторинних серверів або коли вторинні сервери потрібно повторно синхронізувати після тривалого простою.

Додаткові передачі зон містять лише зміни в зоні з часу останньої передачі. Оскільки їм потрібна менша пропускна здатність і обчислювальна потужність для підтримки процесів синхронізації, поступові передачі зон можуть бути корисними в динамічних зонах, які часто змінюються.

Відмітимо переваги зон DNS:

децентралізація. Організації можуть використовувати різні зони для розподілу адміністративного навантаження, пов'язаного з доменом, і запобігання

перевантаженню будь-якого конкретного адміністратора або сервера;

адміністративна автономія. Організації можуть використовувати зони DNS, щоб отримати більш детальний контроль над керуванням записами DNS і розподілом трафіку. Ця можливість дозволяє організаціям керувати записами DNS відповідно до своїх унікальних потреб, не чекаючи, поки зміни поширяться через центральну систему;

розподіл навантаження. Зони DNS полегшують розподіл інтернет-трафіку між різними серверами, дозволяючи адміністраторам зони налаштовувати власні параметри DNS для балансування навантаження та відновлення після відмови;

швидкість. Делегування повноважень у межах зон означає, що DNS-перетворювачі можуть зменшити кількість переходів, необхідних для визначення доменного імені, що в кінцевому підсумку прискорює процеси маршрутизації та отримання даних.

Для налаштування основних зон використовується Akamai Control Center або Edge DNS Zone Management API, щоб виконати початкове налаштування служби Edge DNS.

Edge DNS Zone Management API також включає операції масової зони та операції, які дозволяють отримувати дані про корпоративну конфігурацію Edge DNS.

Розглянемо робочий процес для налаштування основної зони. Необхідно виконати наступні кроки, щоб налаштувати основні зони за допомогою Akamai Control Center:

1. додайте основну зону DNS;

2. додайте новий набір записів;

3. перегляньте та надішліть список змін.

Розглянемо порядок додавання основної зони DNS.

Первинні зони DNS дозволяють Akamai обслуговувати записи DNS корпоративних доменів без необхідності підтримувати власні головні сервери DNS.

Необхідно мати на увазі, що додаючи основну зону, яка є підзоною. Якщо ми

додаємо основну зону, яка є підзоною наявної вторинної зони, вміст основної зони, яку ми створюємо, може замінити вміст вторинної зони. Будьте обережні, щоб переконатися, що в просторі імен між існуючою вторинною зоною та новою основною зоною немає конфліктів.

Щоб додати основну зону DNS, виконайте наступну процедуру:

1. увійдіть до Центру керування;

2. перейдіть до ☰ > DNS SOLUTIONS > Edge DNS. Відкриється сторінка списку зон;

3. на верхній панелі інструментів натисніть «Додати зону»;

Якщо «Додати зону» виділено сірим кольором, ми досягли максимальної кількості виділених зон. Щоб збільшити ліміт, зверніться до представника сервісної служби.

4. на сторінці «Додати зону» налаштовуємо параметри основної зони. використовуючи наведені нижче описи полів як вказівки:

5. щоб увімкнути передачу вихідної зони, перегляньте розділ «Увімкнення передачі вихідної зони»;

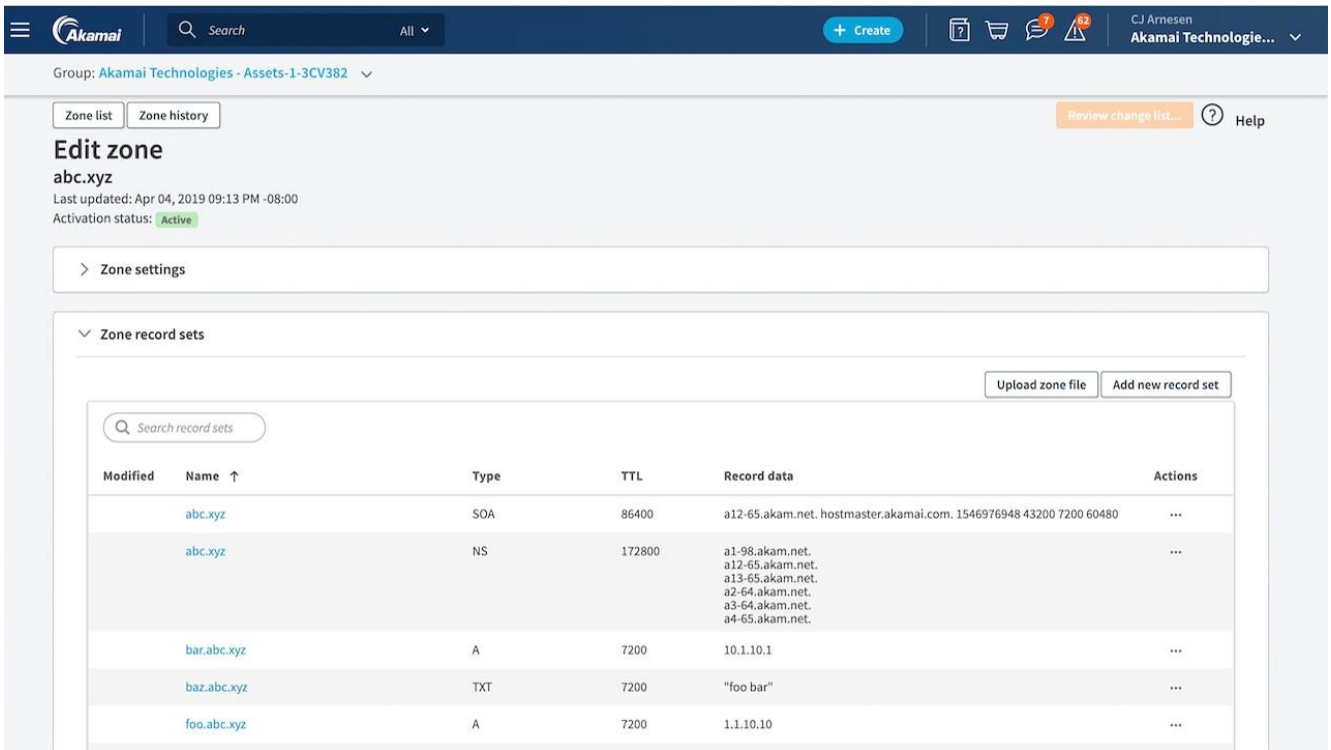

Рис. 3.1. Інтерфейс Akamai Control Center

6. натисніть «Створити зону». З’явиться сторінка редагування зони нової зони.

7. додайте новий набір записів.

Розглянемо робочий процес для налаштування вторинної зони. Для цього використовується Akamai Control Center або Edge DNS Zone Management API, щоб виконати початкове налаштування служби Edge DNS:

1. увійдіть до Центру керування;

2. перейдіть до ☰ > DNS SOLUTIONS > Edge DNS. Відкриється сторінка списку зон;

3. на верхній панелі інструментів натисніть «Додати зону»;

Якщо «Додати зону» виділено сірим кольором, ми досягли максимальної кількості виділених зон. Щоб збільшити ліміт, зверніться до представника сервісної служби.

4. на сторінці «Додати зону» налаштовуємо параметри додаткової зони. використовуючи наведені нижче описи полів як вказівки:

5. щоб увімкнути передачу вихідної зони, перегляньте розділ «Увімкнення передачі вихідної зони»;

6. натисніть «Створити зону». Відкриється сторінка «Зведення активних зон» зі списком офіційних серверів імен Akamai та IP-адресами агента передачі зон.

3.2. Порядок контролю та захисту корпоративних зон

Захист зон дає змогу контролювати корпоративні зони на наявність доменів, які загрожують організації. Захист зони відстежує такі загрози [12]:

фішинг. Домени, які використовуються для фішингової кампанії або для підроблених веб-сайтів. Фішингові домени часто використовуються для створення веб-сайтів, які виглядають законними, але насправді обманюють користувачів, змушуючи їх надавати конфіденційну інформацію, як-от облікові дані для входу, дані кредитної картки тощо.

Фішингова атака може бути націлена на користувачів в організації,

надсилаючи підроблені сповіщення, які закликають до негайних дій. Ці шахрайські сповіщення можуть надходити у вигляді електронних листів і використовувати складну тактику залякування. Наприклад, ці повідомлення можуть попереджати про порушення авторських прав або торгових марок у спробі отримати конфіденційну інформацію про організацію. Рішення Akamai відстежує домени, які належать до адрес електронної пошти відправників електронної пошти;

типосквотінг (typosquatting). Домени, які є типовою орфографічною помилкою або неправильним типом іншого популярного домену чи бренду. Хоча typosquatting можна використовувати для дій, які становлять низький ризик для організації, суб'єкти загрози можуть використовувати цю техніку, щоб спрямовувати користувачів на підроблені веб-сайти, призначені для викрадення інформації або встановлення шкідливого програмного забезпечення.

Коли ми вмикаємо захист зони в зоні, рішення Akamai активно стежить за зоною та звітує про домени, які використовуються для цієї зловмисної діяльності.

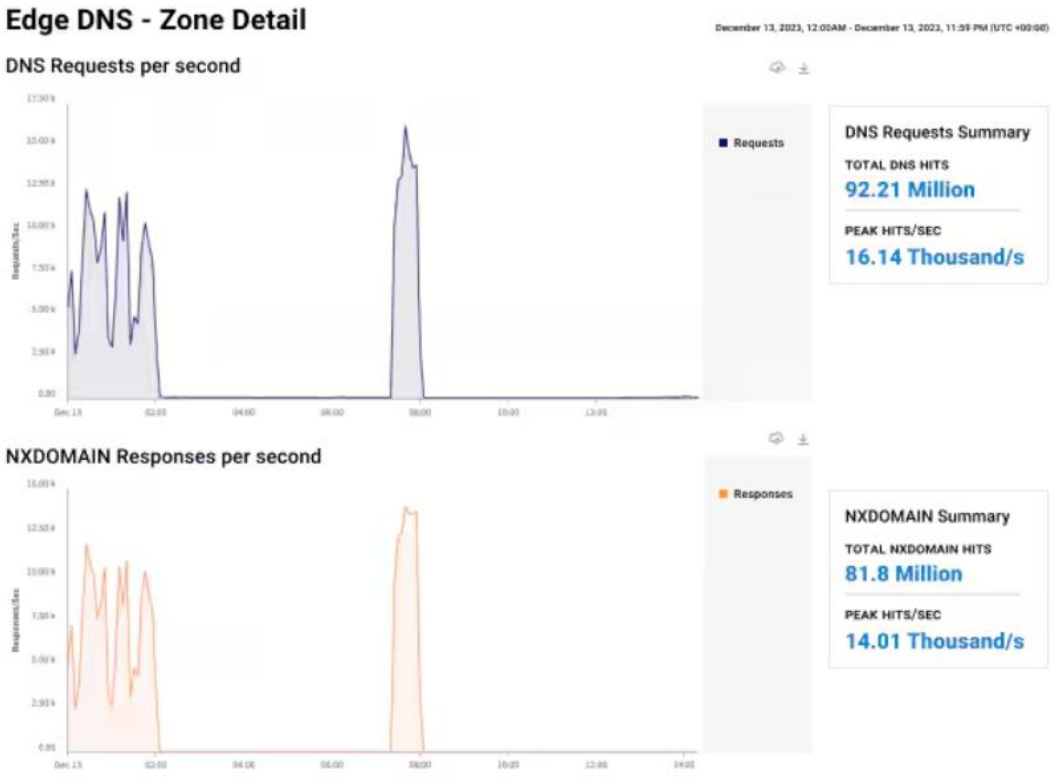

Рис. 3.2. Інтерфейс рішення Akamai Edge DNS

У Центрі керування рішення Akamai ми можемо [12]:

увімкнути зональний захист у кожній із корпоративних зон;

переглянути детальний звіт про домени, які становлять загрозу для організації. Інформація містить індикатори ризику, URL-адреси, де використовувався домен, тощо. Ми можемо фільтрувати домени за рівнем загрози, установлювати рівень пріоритету для доменів, призначати адміністраторів, які мають стежити за доменом, і переглядати звіт;

видалити домени, які становлять ризик для нашої організації;

додати або видалити домени з білого списку. Граничні зони DNS автоматично додаються до білого списку. Домени в цьому списку не відстежуються на наявність фішингових загроз і не включені у звіт про пов’язані домени чи будь-який звіт про зони;

переглянути інформаційну панель, яка дає нам високорівневе графічне представлення зловмисних доменів. Він також показує кількість видалень, які тривають або завершені.

3.3. Рекомендації щодо захисту корпоративної інфраструктури DNS

Безпека DNS передбачає захист інфраструктури DNS від кіберзагроз для забезпечення її швидкої та надійної роботи. Надійна стратегія безпеки DNS включає кілька рівнів захисту, наприклад розгортання резервних DNS-серверів, впровадження протоколів безпеки, таких як DNSSEC, і забезпечення ретельного журналювання DNS.

Для підвищення ефективності захисту корпоративної інфраструктури DNS необхідно:

зміцнювати свою безпеку, розширивши знання про інструменти DNS і відчутні переваги від даних DNS, які можна використовувати. Використання спеціалізованого рішення для аналізу загроз, орієнтованого на DNS, дозволяє організаціям проактивно захищати, швидко виявляти та захищати від кіберзагроз;

використовувати DNS, щоб покращити контроль доступу та

мікросегментацію. Включення інструментів безпеки DNS у стратегію нульової довіри гарантує, що доступ до конфіденційних ресурсів мають лише авторизовані користувачі, пристрої та програми;

намагатися раніше виявляти витоки даних і неконтрольовані служби завдяки видимості DNS, можливості спостереження та інтелектуальній аналітиці. Моніторинг і аналіз трафіку DNS покращує виявлення програм-вимагачів або будь-якої підозрілої мережевої активності та забезпечує відповідність нормативним вимогам;

інтегрувати дані DNS з екосистемою безпеки, щоб підвищити проактивність, автоматизувати реагування безпеки та прискорити усунення загроз. Перехід до більш інтегрованої та цілісної інфраструктури безпеки підвищить загальну ефективність, зменшить складність і покращить рентабельність інвестицій.

В [2] визначені такі заходи для зменшення ризиків безпеки DNS:

необхідно впровадити DNSSEC (розширення безпеки DNS). DNSSEC (Domain Name System Security Extensions) підвищує безпеку DNS , дозволяючи перевіряти дані DNS за допомогою цифрових підписів.

Це гарантує автентичність і цілісність відповідей DNS, запобігаючи атакам підробки DNS і отруєння кешу. DNSSEC працює, підписуючи дані DNS на кожному рівні ієрархії DNS, дозволяючи резолверам перевіряти джерело та цілісність даних.

Найкращі методи роботи з DNSSEC [2]:

підпишіть свої зони DNS: застосуйте цифрові підписи до своїх зон DNS, щоб переконатися в їх автентичності;

увімкнути перевірку DNSSEC: налаштуйте ваші розпізначі DNS для перевірки підписів DNSSEC;

контролюйте та обслуговуйте: регулярно перевіряйте працездатність розгортань DNSSEC і за потреби оновлюйте ключі.

необхідне використання DNS-фільтрації та блокування. Фільтрація та блокування DNS передбачає аналіз запитів і відповідей DNS для виявлення та блокування шкідливих доменів. Це допомагає запобігти доступу до шкідливих

сайтів і зменшує ризик фішингу, зловмисного програмного забезпечення та інших кіберзагроз. Розширені рішення для фільтрації DNS використовують аналіз загроз, щоб не відставати від нових загроз і забезпечити захист у режимі реального часу.

Найкращі методи фільтрації DNS [2]:

використовуйте канали аналізу загроз: інтегруйте аналіз загроз для виявлення та блокування шкідливих доменів;

необхідно впровадити фільтрацію на основі категорій: блокувати цілі категорії шкідливого або небажаного вмісту (наприклад, фішинг, зловмисне програмне забезпечення);

використання політик: налаштуйте політики фільтрації відповідно до конкретних потреб організації та вимог відповідності.

моніторинг і реєстрація трафіку DNS. Безперервний моніторинг і реєстрація трафіку DNS є критично важливими для виявлення підозрілих дій і потенційних загроз. Аналізуючи моделі трафіку DNS, організації можуть виявити аномалії, які можуть свідчити про поточну атаку або спробу викрадання даних.

Найкращі методи моніторингу трафіку DNS [2]:

розгортання інструментів моніторингу: використовуйте інструменти моніторингу DNS для захоплення та аналізу трафіку DNS у режимі реального часу;

використання сповіщення про аномалії: налаштуйте сповіщення про незвичайні дії DNS, такі як стрибки трафіку або несподівані типи запитів;

проводьте регулярні перевірки: регулярно переглядайте журнали DNS, щоб виявити тенденції та потенційні проблеми безпеки.

безпечне налаштування DNS-серверів. Безпечна конфігурація DNS-серверів є важливою для зменшення вразливості та захисту від атак. Це включає впровадження найкращих практик для захисту серверів, контролю доступу та протоколів безпеки.

Найкращі методи конфігурації безпечного DNS-сервера [2]:

вимкнути непотрібні служби: вимкніть непотрібні служби чи функції;

запровадження контролю доступу: обмежте доступ до інтерфейсів керування DNS-сервером лише авторизованому персоналу;

використання безпечних протоколів: використовуйте безпечні протоколи зв’язку, такі як DNS через HTTPs (DoH) або DNS через TLS (DoT), щоб шифрувати трафік DNS.

використання багаторівневих стратегій безпеки. Багаторівневий підхід до безпеки передбачає поєднання різних заходів безпеки для створення надійного захисту від атак DNS. Ця стратегія гарантує, що навіть якщо один шар буде порушено, додаткові рівні захисту зможуть пом’якшити вплив.

Найкращі методи багаторівневої стратегії безпеки [2]:

брандмауери та IDS/IPS: розгорніть брандмауери та системи виявлення/запобігання вторгненням для блокування та виявлення зловмисних дій;

безпека кінцевих точок: захистіть окремі пристрої за допомогою антивірусних засобів і рішень для захисту кінцевих точок;

регулярні оцінки безпеки: проводите регулярні оцінки безпеки та тестування на проникнення, щоб виявити та усунути вразливості.

Вибір правильного програмного забезпечення DNS має вирішальне значення для забезпечення надійної безпеки DNS. Програмне забезпечення має пропонувати розширені функції безпеки, масштабованість і надійність для задоволення потреб конкретної організації.

Оцінюючи програмне забезпечення DNS, враховуйте такі фактори, як:

можливості виявлення загроз;

простота управління;

інтеграція з іншими засобами безпеки.

ВИСНОВКИ

В роботі досліджено проблему захисту корпоративної інфраструктури DNS, визначено його мету та завдання. Захист DNS-серверів є критично важливим бізнес-пріоритетом для команд безпеки організацій. Оскільки DNS дозволяє корпоративним користувачам отримувати доступ до веб-додатків і API організації, будь-яка загроза корпоративним DNS-серверам також є загрозою бізнес-операціям, прибутковості та довірі клієнтів і партнерів.

Забезпечення конфіденційності, автентичності інформації та підтримання цілісності інформації, що передається, має вирішальне значення для ефективного функціонування Інтернету, для якого DNS надає службу розпізнавання імен, є головними цілями захисту корпоративної інфраструктури DNS.

Визначено існуючі підходи до захисту корпоративної інфраструктури DNS. Основними підходами, які можна використовувати для захисту DNS, є DNS захист від DDoS, інструмент безпеки DNSSEC, DNS-фільтр, брандмауер тощо.

Проаналізовано методи та засоби захисту корпоративної інфраструктури DNS на базі Akamai Edge DNS. Продукт Akamai Edge DNS – це хмарне рішення, яке забезпечує доступність 24/7, покращує швидкість реагування та покращує стійкість DNS-серверів, оскільки вони захищаються від найбільших DDoS-атак.

Визначено призначення, основні функції та склад рішення Akamai Edge DNS. Akamai Edge DNS – це авторитетна служба DNS. Це рішення забезпечує безпечну, високопродуктивну, масштабовану та високодоступну граничну службу для авторитетного DNS. Akamai Edge DNS використовує глобальне розгортання Akamai тисяч серверів імен у кількох мережах, використовує IP Anycast і покладається на власну реалізацію протоколу DNS як загального компонента Akamai Intelligent Platform.

На основі досліджень проведених в роботі запропоновано порядок застосування технології захисту корпоративної інфраструктури DNS на базі Akamai Edge DNS. Розглянуто порядок застосування рішення Akamai Edge DNS, а

також порядок контролю та захисту корпоративних зон. Розроблено рекомендації фахівцям з кібербезпеки щодо захисту корпоративної інфраструктури DNS.

Таким чином, правильна реалізація технології захисту корпоративної інфраструктури DNS має забезпечити ефективний захист корпоративних даних та кібербезпеку інформаційної системи організації.

ПЕРЕЛІК ПОСИЛАНЬ

1. Romain Fouchereau. 2023 Global DNS Threat Report. IDS. URL: https://efficientip.com/wp-content/uploads/2023/09/IDC-2023-DNS-Threat-Report.pdf

2. The Most Common DNS Security Risks in 2024 (And How to Mitigate Them). Heimdal. Last updated on July 30, 2024. URL: https://heimdalsecurity.com/blog/dns-security-risks/

3. Understanding DNS Security Threats and How to Mitigate Them. Pathways, Feb 26, 2024. URL: https://www.ippathways.com/understanding-dns-security-threats-and-how-to-mitigate-them/

4. Alex de Oliveira. How do DNS-based threats affect your business? Lumiun Blog, January 24, 2024. URL: https://www.lumiun.com/blog/en/how-dns-based-threats-affect-your-business/

5. What Is DNS Security? Akamai. URL: https://www.akamai.com/glossary/what-is-dns-security#accordion-18c62ed225-item-762c0f1dd4

6. Security Of The Domain Name System (DNS). An Introduction For Policy Makers. OECD Digital Economy Papers, October 2022 No. 331. URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/10/security-of-the-domain-name-system-dns_1fac3ffa/285d7875-en.pdf

7. What is DNS security? Cloudflare. URL: https://www.cloudflare.com/learning/dns/dns-security/

8. Best Practices Guide: DNS Infrastructure Deployment. BlueCat. URL: https://bluecatnetworks.com/wp-content/uploads/2020/06/DNS-Infrastructure-Deployment.pdf

9. Ramaswamy Chandramouli, Scott Rose. Secure Domain Name System (DNS). Deployment Guide. NIST Special Publication 800-81-2. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-81-2.pdf

10. DDoS Protection. Reference Architecture. Akamai. URL: https://www.akamai.com/resources/reference-architecture/ddos-protection

11. What Are DNS Servers? Akamai. URL: https://www.akamai.com/glossary/what-are-dns-servers

12. Welcome to Edge DNS. Akamai. URL: https://techdocs.akamai.com/edge-dns/docs/welcome-edge-dns

13. AKAMAI Product Brief. Edge DNS – Comprehensive DNS Security Akamai. URL: https://www.akamai.com/resources/product-brief/edge-dns

14. Chrystal R. China, Michael Goodwin. What is a DNS zone? IBM, Published: 7 June 2024. URL: https://www.ibm.com/topics/dns-zone

15. Лисаченко Аліна В'ячеславівна, Технологія захисту корпоративної інфраструктури DNS на базі Akamai Edge DNS. Всеукраїнська наукова конференція «Актуальні проблеми кібербезпеки». Державний університет інформаційно-комунікаційних технологій. 25 жовтня 2024. Тези доповідей. С. 113-116. URL: https://duikt.edu.ua/uploads/p_2661_48963150.pdf

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)